

워크숍 자료집

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

제1차 2016. 3. 25
제2차 2016. 4. 29
제3차 2016. 5. 27
제4차 2016. 6. 27
제5차 2016. 9. 26



한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

2016년도 기본과제
워크숍 자료집

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

제1차	2016. 3. 25
제2차	2016. 4. 29
제3차	2016. 5. 27
제4차	2016. 6. 27
제5차	2016. 9. 26



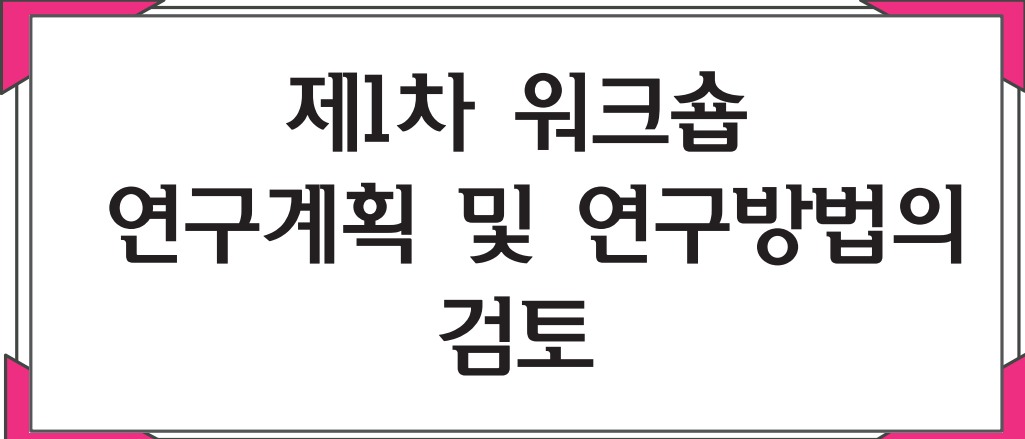
한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

전체 목차

■ 제1차 워크숍: 연구계획 및 연구방법의 검토	7
□ 연구계획서	11
□ 자문의견서	23
○ 의견1 (강영기)	25
○ 의견2 (권건보)	31
○ 의견3 (김일환)	35
○ 의견4 (김현경)	39
○ 의견5 (오태원)	41
○ 의견6 (정소영)	43
■ 제2차 워크숍: 생체정보의 활용 현황에 관한 검토(1) - 바이오인식분야-	47
□ 발 제 문	53
○ 생체인증(바이오인식 인증)을 이용한 인증기술 및 시장현황 (이승재)	55
○ 생체정보의 활용현황 - 바이오인식기술 (전동훈)	69
○ 바이오인식 기술의 발전 및 침해 요소 (김건우)	83
□ 토 론 문	87
○ 토론문1 (정필운)	89
○ 토론문2 (방동희)	95
○ 토론문3 (정소영)	97
○ 토론문4 (황현영)	101

■ 제3차 워크숍: 생체정보의 활용 현황에 관한 검토(2)	
- 금융, 의료, 형사수사 분야-	105
□ 발 제 문	111
○ 생체정보의 분야별 활용현황 - 금융, 의료, 수사 분야 (이창범)	113
○ 생체정보의 활용 및 보호를 위한 법제 정비방안 연구 : 생체정보의 분야별 활용현황-의료분야 (배현아)	127
○ 생체정보의 분야별 활용현황 - 범죄수사 분야 (정소영)	147
□ 토 론 문	163
○ 토론문 (김종배)	165
■ 제4차 워크숍: 주요 외국의 생체정보 관련 법제 동향	169
□ 발 제 문	175
○ 독일의 생체정보 관련 법제 동향 (김영미)	177
○ 프랑스의 생체정보 관련 법제 동향 (오승규)	189
○ 미국의 생체정보 관련 법제 동향 (이상경)	199
○ 일본의 생체정보 관련 법제 동향 (강영기)	225
□ 토 론 문	237
○ 토론문 (손형섭)	239

■ 제5차 워크숍: 생체정보의 활용 및 보호를 위한 법제 정비방안	247
□ 발 제 문	253
○ 바이오인식시스템 보안위협과 차세대 Medical biometrics (김재성)	255
○ 생체인식 정보의 처리에 관한 개인정보 보호법제의 현황과 개선방향 (이은우)	279
□ 토 론 문	295
○ 생체정보의 현황(패러다임 변화) 및 입법 전략에 대한 고찰 (방동희)	297



**제1차 워크숍
연구계획 및 연구방법의
검토**

2016. 3. 25.

목 차

□ 연구계획서	11
□ 자문의견서	23
○ 자문의견 1 (강영기)	25
○ 자문의견 2 (권건보)	31
○ 자문의견 3 (김일환)	35
○ 자문의견 4 (김현경)	39
○ 자문의견 5 (오태원)	41
○ 자문의견 6 (정소영)	43

연구 계획서

■ 연구과제명

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

■ 연구책임자

김현희 (사회문화법제연구실 연구위원)

과제구분	기초 <input type="checkbox"/> 정책 <input checked="" type="checkbox"/>
구분 선정 사유	<ul style="list-style-type: none"> ○ 생체정보의 활용은 생체인식 기술의 발전을 전제로 하고 있으며, 생체인식 기술의 발전은 과학기술혁신 역량 강화 및 관련 산업의 발전을 촉진하는 효과가 있으나, 그와 동시에 생체정보의 활용으로 인한 개인정보 침해의 가능성도 상당하므로 이를 방지하고 개선하기 위한 법제개선방안을 제시

■ 관련 정책현안 및 연구의 필요성

1. 개념

- 생체정보(Biometric Information)는 지문, 홍채, 망막, 얼굴, 음성, 손모양, 손혈관, 서명 등을 개인의 일정한 생체적 특성들을 측정 한 후 이를 데이터베이스화하고 이를 통하여 그 개인을 인식하는 이른바 생체인식기술을 기반으로 다방면에서 활용되고 있음
- 생체적 특성은 크게 신체적 특성과 행동적 특성으로 구분할 수 있으며, 신체적인 특성으로서 지문, 손모양, 얼굴, 홍채, DNA 등이 활용되고 있고, 행동적인 특성으로서 성문(聲紋), 서명, 걸음걸이 등이 활용됨

2. 특징

- 생체정보는 개인정보이지만, 비밀번호, 주민번호, 주소 등의 기존의 개인정보와 달리, 살아있는 동안은 그 사람과 불가분으로 결합되어 있고, 일부 생체정보는 이름, 식별번호 등과 달리 절대적으로 변경할 수 없다는 특수성을 지님

3. 법적 쟁점

- 생체정보는 그 “활용”과 “보호(보안)”에 관한 양 측면 모두에서 논의될 필요가 있음
- 우선, 생체정보의 “활용”과 관련하여서는 2008년 여권법의 전부 개정 시 이슈가 된 이래로 최근 전자금융거래 시 공인인증을 대신하는 본인인증 방식으로서 논의되고 있으며, 빅데이터 환경에 있어서 u-헬스케어(의료기기 등)의 대상정보 기타 범죄수사 등에 있어서 적극적으로 활용되고 있음
- 반면, 생체정보의 “보호”와 관련하여서는 개인의 고유정보이자 민감정보인 생체정보가 유출되거나 악용(위·변조) 되는 경우, 정보주체의 법률관계가 심각하게 침해될 수 있기 때문에 생체정보의 수집, 관리, 폐기에 이르는 전 과정을 신중하게 관리하고 보장하여야 하는 개인정보 내지 프라이버시 보호가 강하게 요청되고 있음
 - 생체정보의 보호 또한 생체정보의 활용의 전제 하에서 그 정의와 범위를 어떻게 보느냐에 따라 달라져야 할 것이기 때문에, 개별 활용분야에서 필요한 보호수준을 정하는 것이 현실적인 방안이 될 수 있음
- 요컨대, 생체정보의 활용 및 보호는 그 범위 및 한계를 논하기 위하여 개별 분야별로 고찰될 필요가 있는데, 크게 생체정보별로 “지문”, “안면”, “홍채”, “성문” 등이 현재의 기술수준에서 어

떻게 활용되고 있는지, 또한 활용분야별로 “금융”, “디지털 헬스케어 서비스”, “출입국”, “복지행정”, “범죄수사” 등의 분야에서 어떠한 생체정보가 어떻게 활용되고 있는지 그 현황을 살펴보고 활용에 대한 규범적 한계 및 보호의 수준 등에 대한 규범적 쟁점을 찾는 것이 시급하다고 판단됨

4. 결론

- 생체정보의 활용 및 보호와 관련하여서는 생체인식의 기술적 발전을 충분하게 지원함과 동시에 유출 및 부정이용에 대한 철저한 보안, 보호를 가능할 수 있게 하는 제도적 환경이 마련되어야 할 필요성이 있음
- 현재 우리 법제에서는 생체정보에 대한 정의가 명확하지 않기 때문에, 활용이나 보호에 관한 규율체계를 설계하기가 어려운 상황이기 때문에 전반적인 방향에서 개선이 요구되고 있음
- 생체정보에 관한 독자적인 법령을 제정하는 것이 가장 이상적일 것이나 규율대상을 정하는 것이 현실적으로 매우 어렵기 때문에, 현행 개별법의 개선방향 내지 개정안을 도출하는 것으로 하고자 함

▣ 연구 목적

- 생체정보가 논의되는 다양한 영역에 대한 연구를 통해 생체정보의 개념과 성격을 정확하게 이해하고, 그 유형 및 범위를 명확히 하며, 그러한 특수한 성격의 정보에 대한 수집, 활용 및 보호에 대한 규범적 기초를 마련함으로써 생체정보 활용기술의 발전을 도모함과 동시에 생체정보의 보호 등을 통한 개인의 자유를 보호하기 위한 적절한 균형점을 모색하는 것을 목적으로 함

■ 선행연구 현황 및 선행연구와 본연구의 차별성

구 분	선행연구와의 차별성			
	연구목적	연구방법	주요연구내용	
주요 선행 연구	1	<ul style="list-style-type: none"> - 과제명 : 생체정보 프라이버시의 쟁점 및 정책 시사점 - 연구자 : 박정훈/김행문(2008) - 연구목적 : 전자여권 도입과정에서 사회적 갈등의 핵심으로 부각되고 있는 생체정보 및 생체정보보호와 관련된 주요 쟁점 분석 	<ul style="list-style-type: none"> - 문헌연구 - 사례조사 및 분석 	<ul style="list-style-type: none"> - 생체정보에 관한 이론적 논의 - 생체정보 보호를 위한 쟁점 연구 - 생체정보 쟁점에 관한 사례분석 연구: 전자여권
	2	<ul style="list-style-type: none"> - 과제명 : 국내의 개인정보보호 정책 비교 분석 - 연구자 : 정대경(2012) - 연구목적 : 개인정보보호정책에 대한 비교연구를 통하여 국가별 개인정보보호정책의 현황을 분석하고 개인정보보호를 강화하기 위해 필요한 정책적 과제를 검토 	<ul style="list-style-type: none"> - 문헌연구 - 사례조사 및 분석 - 비교법연구 	<ul style="list-style-type: none"> - 개인정보보호의 정의와 필요성 - 우리나라의 개인정보 보호정책 - 개인정보보호법 제정 및 주요내용 - 우리나라 개인정보보호 전담조직 - 해외 주요국 개인정보보호 정책
	3	<ul style="list-style-type: none"> - 과제명 : 생체정보보호법제 정비방안에 관한 고찰 - 연구자 : 김일환(2006) - 연구목적 : 생체인식 기술의 발전으로 인하여 나타날 수 있는 문제점을 방지, 해결하기 위하여 각국의 생체정보와 관련한 사례 및 정책, 법제 등 연구 	<ul style="list-style-type: none"> - 문헌연구 - 사례조사 및 분석 - 비교법연구 	<ul style="list-style-type: none"> - 정보사회에서 생체정보의 의의 - 미국과 독일 생체인식정보보호 법제 - 현행 개인정보보호법제의 정비의 필요성과 법안의 검토 - 현행 개인정보보호법제를 통한 생체정보보호여부 검토 - 생체정보보호법에 담길 내용에 관한 고찰
본 연구	<ul style="list-style-type: none"> - 생체정보와 관련한 법제적 문제점들을 전반적으로 살펴보고, 생체정보의 활용 및 활성화, 그에 따른 문제점 등을 파악하여 생체인식기술의 발전과 정보보호 사이에서 나타날 수 있는 모순점에 대한 대책을 마련하고자 함 - 동 연구 관련분야는 급변하므로, 선행연구의 시의성 부족한 것 보완 	<ul style="list-style-type: none"> - 문헌연구 - 사례조사 - 비교법연구 - 전문가자문 	<ul style="list-style-type: none"> - 생체정보의 의의 및 활용현황 - 주요국가 생체정보활용실태 및 법제 - 우리나라의 생체정보와 관련한 법제현황 - 생체정보의 활용 및 보호를 위한 법제개선 방안 - 선행연구 비교법 조사가 간단하고 불충분하며, 시일이 경과하여 해당국도 상당한 변화가 있었을 것을 반영함 	

▣ 주요 연구내용

제1장 서론

제1절 연구의 필요성 및 목적

제2절 연구의 범위 및 방법

제2장 생체정보의 의의 및 활용 현황

제1절 생체정보의 개념, 유사개념과의 차이

제2절 생체정보의 성격 및 특성

제3절 생체인식 기술의 발전과 생체정보의 활용

- 정보별 활용현황 : 지문, 홍채, 안면, DNA, 성문 등
- 분야별 활용현황 : 금융, 출입국, 디지털헬스케어, 행정(복지 등), 범죄수사 등

제3장 생체정보 관련 법제 현황 및 문제점

제1절 현행 개인정보 및 생체정보 관련 법제 현황

- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「개인정보보호법」, 「전자금융거래법」, 「전자서명법」, 「여권법」 등

제2절 현행 법제의 문제점

- 기존 법제의 한계 : 생체정보의 규범적 정의 내지 적용범위 등에 따른 활용과 보호의 한계
- 생체인식 산업발전과 개인정보보호 간 법익 긴장, 충돌, 공백에 관한 문제점

제4장 주요 국가의 생체정보 관련 규범

제1절 OECD : 프라이버시보호와 개인데이터의 유통에 관한 가이드라인

제2절 EU : 개인정보의 처리에 관한 개인의 보호와 개인정보의
자유이동을 위한 준칙

제3절 개별 국가의 생체정보 관련 법제 : 미국, 프랑스, 독일, 일
본 등 최신 입법동향

제4절 시사점

제5장 결론

제1절 연구의 요약

제2절 생체정보의 수집, 활용 및 보호를 위한 법제 개선방안

▣ 연구추진방법

- 문헌연구 및 실태조사
- 연혁분석 및 법제 분석
- 선진국가의 사례 및 법제 분석
- 전문가 회의 및 워크숍 개최
- 법제정비 실무전문가협의회 추진
- 관련부처(금융위원회, 행정자치부, 미래창조과학부) 실무전문가
초빙 전문가회의
- 학계 법제정비 전문가협의회 구성

▣ 관련부처 및 국정과제 관련성

- 정책수요처(정부, 기관 등)
 - 행정자치부, 미래창조과학부, 법무부, 금융위원회, 한국인터넷진흥원 등

- 국정과제 관련성

국정 기조	추진전략		국정과제	
	코드	명	코드	명
1	1-1	창조경제	1-1-8	과학기술을 통한 창조경제 기반 조성
			1-1-19	혁신적인 정보통신 생태계 조성
2	2-6	국민안전	2-6-81	개인정보보호 강화

▣ 기대효과

- 예상되는 학술적 기여도
 - 생체정보 분야의 입법체계 정비방안 제시를 통한 우리나라 인권 분야의 정책적 체계를 정립할 수 있을 것으로 기대

- 예상되는 정책적 기여도
 - 생체정보 활용 확산에 따른 프라이버시 침해 및 인권침해에 대한 법제적 대응방안 마련
 - 생체정보 악용을 막기 위한 생체정보의 수집, 관리, 폐기에 따른 과정에 대한 법제적 대응 방안 마련

■ 연구기간

연구년차	(1년차/신규)	연구기간	10개월	시작일	2016.01.01.	종료일	2016.10.31
------	----------	------	------	-----	-------------	-----	------------

■ 기타 참고사항 : “개인정보”(생체정보)에 관한 규범적 정의

(1) 생명윤리 및 안전에 관한 법률

- 유전정보란 인체유래물을 분석하여 얻은 개인의 유전적 특징에 관한 정보를 말한다(제2조제14호).
- 개인식별정보란 연구대상자와 배아·난자·정자 또는 인체유래물의 기증자(이하 연구대상자등이라 한다)의 성명·주민등록번호 등 개인을 식별할 수 있는 정보를 말한다(제2조제17호).
- 개인정보란 개인식별정보, 유전정보 또는 건강에 관한 정보 등 개인에 관한 정보를 말한다(제2조제18호).

(2) 개인정보보호법

- 개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다(제2조제1호).
- 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다(제23조전문).

(3) 보건의료기본법

- 보건의료정보란 보건의료와 관련한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료를 말한다(제3조제6호).

(4) 의료법

- 전자의무기록(제23조제3항) : 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.

(5) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

- 개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다(제2조제6호).

(6) 전자서명법

- 개인정보라 함은 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다(제2조제13호).

(7) 전자금융거래법

- 접근매체라 함은 전자금융거래에 있어서 거래지시를 하거나 이용

자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다(제2조제10호).

가. 전자식 카드 및 이에 준하는 전자적 정보

나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조 제7호의 인증서

다. 금융회사 또는 전자금융업자에 등록된 이용자번호

라. 이용자의 생체정보

마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

(8) 신용정보의 이용 및 보호에 관한 법률

- 개인식별정보(제34조제1항) : 신용정보제공·이용자가 개인을 식별하기 위하여 필요로 하는 정보로서 대통령령으로 정하는 정보(이하 개인식별정보라 한다)를 신용정보회사등에 제공하려는 경우에는 해당 개인의 동의를 받아야 한다.

자문의견서

의견 1

강 영 기
(고려대 법전원 연구교수)

▣ 검토 및 자문사항

1. 연구의 방향과 범위

- 생체정보의 “활용”과 “보호”에 관한 연구가 한꺼번에 가능한지?
활용은 ‘편리성중시’ vs 보호는 ‘안전성중시’의 trade-off 관계에 있고
필연적으로 양자는 함께 논의하지 않으면 안 될 듯

- 보고서 체재는?

주기별(수집, 활용, 보호 등)로 나눌 것인가? vs. 분야별(의료, 출입
국, 본인인증, 범죄 등)로 나눌 것인가? 아니면 다른 구분?

결국은 개인정보보호법제로 귀결된다고 하면 제도 도입의 운용을
위한 규범체계가 어떠한 형태를 가지는 것이 바람직한지도 논의할 필
요가 있다.

예컨대 가이드라인 중심의 규율논의 vs. 입법을 통한 규제의 형태

* 의료와 관련하여 환자의 기록에 대한 프라이버시권도 중요하지만...

* 가장 필요한 부문은 금융범죄방지와 정보보안조치의 향상방안?

* 테러의 사전방지를 위한 규정의 정비로서 출입국관리법 등의 개
정도 현실적으로 필요?

: 생체정보의 활용주체와 활용영역에 따라 그 생체정보의 보호의
정도와 범위가 달라질 수 있으므로 활용영역을 어떻게 구분할
수 있을지를 정하고 구체적인 영역별 생체정보의 활용범위와 보
호범위를 생각하는 것도 하나의 방법이 아닐까 생각한다.

2. “생체정보”의 의의

- 생체정보의 개념은? (연구계획서 5페이지의 ■ 기타 참고사항 참고)

생체적인 특징과 특성을 총칭하여 생체정보라고 하는데, 이에 는 지문이나 얼굴 등 신체적 외관에 의한 신체적 특징과 음성이나 서명 등 행동 특성에 따른 행동적 특징이 있다. 신체적 특징은 항상 본인의 육체에 붙어있고 행동적 특징은 본인의 버릇이므로 본인이라면 재현이 가능하다.

생체정보는 개인정보 중 특정개인을 식별할 수 있는 생체정보와 통계자료로서의 활용을 위해 가공된 일종의 데이터로서의 식별가능성이 배제된 생체정보로 나눌 수 있을 것. 후자의 경우는 프라이버시권의 침해가능성이 거의 없으므로 보호의 필요성이 낮을 것이다.

- 기존 “개인정보” 등과의 차이, 구별실익은?

개인정보는 생존하고 있는 개인에 관한 정보로서 당해 정보에 포함되는 성명, 생년월일 기타 기술 등에 의해 특정의 개인을 식별할 수 있는 정보를 가리키는데(개인정보보호법 2조(정의)1항), 이로써 개인을 특정할 수 있고 다른 정보와 조합하면 쉽게 개인을 특정할 수 있다. 즉, 개인정보란 특정개인의 식별정보이다. 개인정보의 대부분은 특정인의 식별가능성이 있으므로 프라이버시권적인 성격을 가진다.

개인정보 중에서 생체적인 특성을 통한 특정개인의 식별가능성을 가진 정보가 생체정보라고 할 수 있으므로 생체정보의 범위가 더 좁다고 할 수 있다.

- 생체정보의 개념을 어떻게 보느냐(정의 내지 범위)에 따라 본 연구의 목적이나 방향이 많이 달라지게 되는지?

생체정보는 다양한 용도로 활용될 가능성이 있는데, 예컨대 개호복지, 재해대응, 디지털건강관리 등에도 이용될 수 있으므로 생체정보의

집약관리를 위한 정보보호기술의 개발, 생체정보를 운용하기 위한 구조 등이 필요할 것이다. 그리고 DNA정보의 인증이 제품화되어 실용화 단계에 접어들었다는 얘기도 있는데, 생체정보의 인증도입과 운용단계에서는 안전성과 편리성의 균형이 중요하다. 그리고 생체정보의 활용을 위한 목적에 따라 생체정보 보호의 범위와 정도가 달라질 것이다.

3. 현행 법제의 문제점

- 구체적인 쟁점사항은? (2000년대 초반의 논의는 요약정리로 대체)
- 기술방법에 대한 의견은?
 - 우선 생체정보의 활용목적에 따라 적용분야를 구분하고 생체정보보호의 필요성과 정도 및 범위를 구체화하는 방안을 생각해볼 수 있을 듯.

4. 외국 법제 소개

- 2010년 전후의 국제규범, 외국규범의 추세, 동향은?
 - ① OECD : “프라이버시 가이드라인” 개정요강?
 - ② APEC : CBPR(APEC越境 프라이버시 Rule)제도?
 - ③ EU : 개인데이터보호지침, e-privacy 지침, 개인데이터보호규칙 안?
 - ④ 미국 : 소비자 프라이버시 권리장전, 개별법?
 - ⑤ 일본 : 저출산과 고령화로 인구가 감소하는 상황에서 사회보장과 세제의 일체적 개혁의 일환으로 일반법인 ‘개인정보보호법’이 개정되고 특별법인 ‘My Number법안’, ‘의료개인정보보호법안’ 등을 마련하며 이를 위한 ‘번호정보보호위원회’ 조직을 구성하고, ‘개인정보보호 가이드라인’을 마련하며 문제는 산적하여 있지만 ‘Privacy Mark 제도’와 같은 ‘민간인증제도’에 관한 검토도 진행.

예컨대, 의료관련분야와 관련하여 개인정보를 취급하는 주체와 적용법규, 감독관청을 간단히 보면 다음과 같다.

개인정보 취급주체	적용법규	감독관청
후생노동성	행정기관개인정보보호법	총무성
국립 암 연구센터	독립행정법인 등 개인정보보호법	총무성
岩手(이와테)현립병원	岩手(이와테)현 개인정보보호조례	이와테현
宮城(미야기)현립병원	宮城(미야기)현 개인정보보호조례	미야기현
陸前高田市립병원	陸前高田市 개인정보보호조례	陸前高田市
大船渡市立병원	大船渡市 개인정보보호조례	大船渡市
의료복지법인 濟生會	개인정보보호법	후생노동성
鈴木내과의원	개인정보보호법	후생노동성

- 소개 필요성이 있는 국가는?

일본에서는 2005년 4월 1일 전면 시행되었던 개인정보보호법의 개정법이 2015년 9월 3일 중의원 본회의에서 가결·성립되어 10년 만에 개정되었다. 이 배경에는 빅 데이터의 활용에 대한 기대가 있다. 네트워크의 발전과 데이터의 축적, 정보처리기술의 발전에 따라 빅 데이터를 분석하여 유익한 정보를 얻는 것이 가능해졌다. 여기에는 인간의 행동 등에 관한 **personal data**도 포함된다. 물론 데이터 활용에 있어서는 소비자에게 불안감을 주지 않도록 할 제도구축이 필요하다.

개정 개인정보보호법은 개인정보의 정의와 범위를 보다 명확히 하고 부정이용에 대한 벌칙을 새로 부가하였다. 그리고 개인을 특정할 수 없도록 적절히 가공한 경우는 본인의 동의 없이 빅 데이터의 분석결과 등을 제3자에게 제공할 수 있도록 하였다. 따라서 빅 데이터를 활용한 신규 비즈니스를 창출하기 쉬워진다.

한편, 개정 My Number 법(행정절차에서의 특정 개인을 식별하기 위한 번호의 이용 등에 관한 법률)도 있다. My Number제도는 2016년 1

월에 시작하기로 하였는데, 그 사용을 확대하는 법 개정이고 My Number의 당분간 그 용도는 사회보장(연금, 의료, 개호, 복지, 노동보험), 세제(국세, 지방세), 재해대책 분야의 범위이다. 개정법은 2018년부터 사용범위를 확대하는데, 확대되는 사용범위는 ① 금융분야(예금·저금계좌에의 적용, 개설의 간소화 등) ② 의료분야(특정건강검진, 예방접종기록 등)이고 당분간은 예금·저금계좌와 My Number의 조건부 등록은 예금자의 임의사항이다.

총리관저의 IT종합전략본부는 2015년 5월 20일에 My Number 등 분과회 제9회 회합을 개최하고 My Number 제도의 활용추진 로드맵을 제시하였다. 우선 개인번호카드의 공적 개인인증 활용을 변혁의 단초로 하고 2020년에는 카지노 출입규제, 올림픽경기장 출입규제 등에 활용하자는 의견도 있었다.

My Number의 인증에 있어서는 3가지 편리성 향상단계가 제시되었다.

제1단계는 하나의 카드화인데, 개인번호카드로 신용카드, 현금카드, 포인트 카드, 진찰권 등을 통합한다.

제2단계는 스마트기기화인데, 스마트폰 등의 디바이스에 다운로드하여 대용할 수 있도록 연구자 및 관계자와의 협의를 통해 실현한다.

제3단계는 생체정보화인데, 미리 본인확인을 거쳐 등록한 생체정보로 대용하는 것도 가능하게 하는 단계로서 개인번호카드도 스마트폰도 불필요하다.

위와 같은 개정 My Number법과 개정 개인정보보호법은 최첨단의 IT security 기술이나 안심안전기술과 관련되어 있다.

5. 결 론

- 제1안 : 개별 제정법안 대강 작성(기존 제출법안과의 차별성)

* 생체정보의 활용에 관한 가이드라인을 생각해보고 정보보호와 관

련된 기존 개별 법률이나 새로운 법률안의 내용과의 조율 내지 조정을 위한 제도정비방안도 생각해 볼 수 있을 것이다.

- 제2안 : 개별 법령의 개정안 제시

생체정보의 보호에 관한 규제보다는 생체정보의 비즈니스적인 활용방안에 중점을 둔다면 개별법령의 조율이 필요한 부분도 있을 듯하다.

의견 2

권 건 보
(아주대학교 법학전문대학원 교수)

▣ 검토 및 자문사항

1. 연구의 방향과 범위

- 생체정보의 “활용”과 “보호”에 관한 연구가 한꺼번에 가능한지?
 - 생체정보의 무분별한 활용으로 인한 인권 침해의 위험성이 매우 큰 만큼 생체정보의 보호에 만전을 기할 필요가 있음.
 - 하지만 생체인식 기술의 발전은 인류에게 다양한 방면에서 크나큰 편익을 가져다줄 것으로 기대되는 상황에서 생체정보 활용의 길을 전적으로 차단하는 것은 결코 바람직하지 않음.
 - 따라서 생체정보의 “활용”과 “보호”를 적절히 조화하는 방향으로 법제도를 정비해야 할 필요성이 있음.
 - 이러한 점에서 생체정보보호론자들이 주장하는 바도 생체정보의 절대적 활용 반대가 아니라, 생체정보의 ‘적정한 활용’ 내지 생체정보의 ‘적정한 보호’를 지향하는 것이라 할 수 있음.
 - 이에 따라 생체정보의 절제된 활용, 즉 정보주체의 권리를 침해하지 않는 한도 내에서의 생체정보 활용이 요구되는 것이고, 이는 생체정보의 적정한 보호의 수준을 법적으로 강구해야 한다는 요청으로 나타남.
 - 요컨대 생체정보 보호의 ‘적정한’ 수준을 확보하는 것은 동시에 생체정보의 ‘적절한’ 활용 가능성을 법적으로 보장하는 것이기도 함.
 - 이러한 측면에서 생체정보의 “보호”는 생체정보의 “활용”와 분리되어 연구될 수 있는 성질의 것이 아니라, 반드시 상호간의 연관

성 속에서 동시에 연구될 수 있고 또 그렇게 해야 할 주제라고 생각됨.

- 다만 생체정보의 활용 증진방안을 모색함에 있어서 특허, 조세, 생명윤리 등의 문제도 생체인식 기술이나 관련 산업의 발전에 위협적 요인이 될 수 있으나, 이들 요인들을 본 연구에서 동시에 검토하는 것은 생체정보의 “보호”와 관련성을 감안할 때 바람직하지 않을 것으로 사료됨.

○ 보고서 체제는?

- 생체정보는 그 종류와 성질이 다양하고, 그 활용분야에 따라 진흥과 보호의 양 측면에서 고려할 사항이 많을 것으로 예상됨.
- 따라서 분야별로 보고서의 체제를 나누어 기술하되, 해당 분야에서 주로 활용될 생체정보를 중심으로 보호의 적절한 수준을 검토하는 것이 바람직할 것으로 생각됨.
- 물론 세부적 검토의 단계에 들어가서 필요에 따라 주기별(수집, 활용, 보호 등)로 서술하는 것은 가능할 것임.

2. “생체정보”의 의의

○ 생체정보의 개념

- 생체정보가 개념상 ‘신체정보’, ‘유전정보’, ‘건강정보’, ‘디엔에이 신원확인정보’, ‘개인정보’ 등과 어떠한 차이가 있는지 검토하는 것은 법적 보호의 범위나 수준을 판단하고 적용의 법령을 결정하는 데 있어서 매우 중요한 의미를 가진다고 봄.
- 생체정보는 개인식별의 가능성이 현재의 기술력 수준에 따라 상대적일 수 있으므로 일률적으로 개인정보의 일종으로 포섭하기는 어려운 문제가 있을 수 있음.

- 또한 생체정보를 ‘건강정보’와 달리 볼 경우 ‘민감정보’로 분류하여 보다 강화된 보호를 피해야 하는 것인지도 함께 검토될 필요가 있다고 생각됨.
- 생체정보의 개념을 명확하게 설정하지 않으면 연구의 범위를 어느 정도로 해야 할지 혼란이 생길 수 있고, 그에 따라 본 연구의 목적이나 방향에도 영향을 미칠 수 있다고 생각됨.

3. 현행 법제의 문제점

- 구체적인 쟁점사항은? (2000년대 초반의 논의는 요약정리로 대체)
 - 현행 「개인정보보호법」은 생체정보의 특성이나 생체인식기술의 특수성을 충분히 고려하고 있지 않고, 개별법에서도 최첨단의 생체인식기술 발전 추세에 부응하지 못하고 있는 상황임.
 - 「바이오정보 보호 가이드라인」도 최신성이 떨어져 새롭게 부각될 입법정책적 수요에 부응하기 어렵고, 생체정보 보호의 실효성을 담보해야 할 특별한 필요에 대처할 수 없는 한계가 있음.
 - 생체정보 관련 기술의 증진 필요성을 고려하여 일반 개인정보와 어떻게 차별화된 규제의 수준을 설정할 것인가가 관건임.
 - 가령 생체정보를 민간정보에 준하여 그 수집단계에서부터 정보주체의 명시적인 동의를 거치도록 할 것인지 아니면 개인정보보호법에서 정한 사유보다 좀 더 폭넓은 허용조건을 인정할 것인지 검토할 필요가 있음.
 - 또한 이용과 제3자 제공 등의 단계에 있어서도 일반적인 개인정보의 경우와 마찬가지로 정보주체의 사전 동의권을 부여할 것인지, 아니면 법적으로 미리 설정한 일정한 조건을 충족하기만 하면 그 처리를 허용하되 정보주체에게 사후적인 통제권을 부여하는 방식으로 규율함이 타당한지에 대한 검토도 필요할 것임.

- 아울러 생체정보의 의학적 활용, 학문연구를 위한 활용, 제3국으로의 전송 등에 관한 법적 쟁점에 대해서도 논의가 필요할 것임.
- 기술방법에 대한 의견은?
 - 적정하다고 생각됨.

4. 외국 법제 소개

- 2010년 전후의 국제규범, 외국규범의 추세, 동향은?
 - 해외의 입법동향과 관련 논의를 중점적으로 소개하고 이를 토대로 국내의 입법정책적 대응방안을 도출할 필요가 있음.
- 소개 필요성이 있는 국가는?
 - 미국, 일본, 영국, 독일 등 EU 주요 국가

5. 결 론

- 현행 개인정보보호법이 생체정보에 관한 일반법으로 기능할 수 있도록 개인정보보호법에 생체정보 관련 일반 규정을 마련하고, 개별 법령에서 생체정보의 이용과 보호에 관한 특별규정을 두는 방안도 생각해볼 수 있음.
- 하지만 생체정보의 특성과 생체인식기술의 개방성, 입법상 규율의 효율성 등을 고려할 때 기존의 관련 법령을 부분적으로 개정하는 것보다 생체정보의 이용과 보호에 관한 개별 법률안을 제정하는 쪽이 과련 입법체계의 정비에 기여하는 바가 더 클 것으로 생각됨.
- 물론 개별 제정법안의 포괄성과 방대성, 연구기간과 연구인력의 제한성 등을 감안할 때 기존 제출법안과 차별성을 갖는 주요 사항들을 중심으로 그 제정법안의 대강을 작성하는 방안(제1안)이 무난할 것으로 보임

의견 3

김 일 환
(성균관대 법학전문대학원 교수)

1. 문제제기

범죄 수사에서 지문 조회나 건물·시설의 출입통제 및 근태관리 등에 활용되어 보편화된 기술로 여겨지고 있는 생체인증이 점차 금융거래나 전자결제는 물론 모바일 및 통신기술의 진화와 함께 사물인터넷(IoT) 기기 등의 분야로 그 활용이 점차 확대되고 있다. 생체인증은 개인의 고유한 생체정보를 개인의 식별 및 인증에 활용하는 기술이다.

현재 애플, 마이크로소프트, 삼성, 알리바바 등 글로벌 ICT 및 유통 업체들이 생체인증 사업에 대한 투자를 늘려 기술 개발을 서두르고 있다.

특히 최근 핀테크, 사물인터넷, 웨어러블, 헬스케어 등 ICT산업이 크게 확대되면서, 생체인증은 다양한 방면에서 활용되고 있다.

하지만 여전히 생체인식 기술은 안전한 보안 인증수단이지만, 생체인증 확산의 걸림돌인 기술적, 환경적, 사회적, 인식적 한계는 아직 존재하고 있다. 특히, 생체인식기술의 활용으로 개인정보침해나 해킹에 의한 유출피해 등이 강하게 제기되고 있다.

세계적으로 생체인증을 활용한 분야의 서비스와 산업이 성장하고 있지만, 기존 산업 환경에서 제정된 개인정보와 프라이버시 관련 규제 및 정책은 아직 기술개발 수준에 따라가지 못하고 있는 실정이다.

2. 보고서 방향과 내용에 대한 검토사항

- 용어사용

먼저 현재 법학이나 사회과학분야에서는 생체정보, 생체인식이란 용어를 사용하고 있으나, ICT 관련 분야에서는 바이오정보란 단어를 사용하는 경향이 있음. 생체실험, 생체인식 등의 단어가 연상시키는 것에 대한 거부감 등으로 인하여 바이오정보란 단어를 사용함. 이에 대한 검토가 필요함.(관련 각종 가이드라인 등도 바이오정보가이드라인 등으로 출간되고 있음)

- 보고서 범위와 내용과 관련하여

생체정보가 보호되어야 합법적으로 활(이)용될 수 있으므로 이에 관한 검토는 크게 필요없다고 생각함

결국 발전하고 있는 생체인식기술과 활용분야에 대한 기술적 검토 및 이에 대한 규범적 판단이 보고서 내용의 핵심이어야 한다고 생각함

이를 위하여 비교법적 검토보다는 현행 우리나라 개인정보보호법제에 대한 분석과 검토에 근거하여 새로운 법률안의 필요성이나 기존 법제의 개정방향과 내용 등을 제시할 필요가 있음

특히 보고서에 담겨야 할 내용으로는

생체인식기술의 발전 및 활용방안에 대한 기술적 접근은 그로 인하여 나타날 수 있는 문제점 - 개인정보침해, 인증기술의 개발 등 - 을 동시에 고려해야만 한다.

이와 관련하여 발전하고 있는 생체인식기술 및 활용분야에 대한 검토와 더불어 생체(바이오)정보의 개념의 설정 등을 보고서에서 중점적으로 다룰 필요가 있다.

이에 따라서 생체인식기술의 발전, 그에 따르는 정보보안, 인증기술, 마지막으로 이의 도입과정에서 드러나는 개인정보침해문제 등을 기술적, 제도적, 법규범적 차원에서 검토하고 이를 입법론적 연구와 연결해야만 한다.

또한 아직 완벽하지 않은 생체인식 기술에 대한 지속적인 연구가 필요하며, 무엇보다 생체인식이 일상화되는 경우, 이러한 정보를 처리하는 기관(국가 등의 공공기관, 인터넷 은행 등을 포함한 민간기관) 등으로부터 보호 등을 검토해야 한다.

의견 4

김 현 경
(서울과기대 IT정책전문대학원 교수)

■ 검토 및 자문사항

1. 연구의 방향과 범위

- 생체정보의 “활용”과 “보호”에 관한 연구가 한꺼번에 가능한지?

생체정보의 활용영역과 활용영역에 있어서 쟁점화 되고 있는 부분에 대한 검토가 이루어져야 하므로 활용과 보호는 불가분의 관계에 있으며 함께 연구해야만 하는 영역이라고 생각됨

- 보고서 체재는?

: 주기별(수집, 활용, 보호 등)로 나눌 것인가? vs. 분야별(의료, 출입국, 본인인증, 범죄 등)로 나눌 것인가? 아니면 다른 구분?

주기별과 영역별을 함께 검토할 수 있다고 보여짐

예를 들어

1. 의료영역

가. 수집 및 이용

나. 제3자 제공

다. 보관 및 파기

2. 출입국 영역

가. 수집 및 이용

나. 제3자 제공

다. 보관 및 파기

.....

2. “생체정보”의 의의

- 생체정보의 개념은? (연구계획서 5페이지의 □ 기타 참고사항 참고)
- 기존 “개인정보” 등과의 차이, 구별실익은?
- 생체정보의 개념을 어떻게 보느냐(정의 내지 범위)에 따라 본 연구의 목적이나 방향이 많이 달라지게 되는지?

생체정보가 가지는 과거와 현재의 차이를 선행적으로 분석할 필요가 있음

- 기존에 생체정보는 의료 및 의료관련 연구에 국한되어 수집 및 활용
- 최근 디지털헬스케어 기술의 발달에 따른 개인의료정보로서의 활용, 인증기술발달에 따른 본인인증방식으로서의 활용, 근태관리를 위한 활용, 유기아동 보호를 위한 활용, 범죄예방을 위한 활용 등 생체정보의 활용이슈는 점차 다각화 되고 있음
- 이러한 환경변화가 부여하는 의미를 선행적으로 분석하고 그 중 특히 문제나 쟁점이 될 수 있는 4~5개 영역을 선정하여 심층분석하는 방식으로 연구를 진행하는 것도 하나의 방안이 될 수 있음

3. 현행 법제의 문제점

- 구체적인 쟁점사항은? (2000년대 초반의 논의는 요약정리로 대체)
- 기술방법에 대한 의견은?

- 영역별로 필요에 의해 유전자정보, 개인정보, 민감정보, 의료정보 등 개별법상의 용어 안에 포함되어 다루어지고 있으며, 별도의 생체정보만의 독자적 규율체계는 없음
- 통일적 규제가 필요한 부분과 영역별 특성이 존중되어야 하는 부분이 존재하는 바 이에 대한 인식을 어느정도 공감하고 논의를 진행할 필요가 있음

의견 5

오 태 원
(경일대학교 경찰학과 교수)

▣ 검토 및 자문사항

1. 연구의 방향과 범위

- 생체정보의 “활용”과 “보호”에 관한 연구가 한꺼번에 가능한지?
개인정보와 관련된 법제에 있어서 보호와 활용은 마치 서로 상충하는 것으로 인식되기도 합니다. 그러나 면밀히 따져보면, 명확한 보호의 영역과 방법을 규정하는 것은 결국 명확한 활용의 영역과 방법을 규정해주는 것이 됩니다. 동전의 양면과 같다고 생각합니다. 물론 연구의 중요한 방향성을 어디에 놓을 것인가에 따라서 보호와 활용의 경계선을 어디에 설정할 것인지에 대하여 차이가 생길 수 있겠습니다만 궁극적으로 보호와 활용의 영역과 방법을 명확하게 규정하는 것은 결국 같은 연구가 될 것이라고 생각합니다.

- 보고서 체재는?

: 주기별(수집, 활용, 보호 등)로 나눌 것인가? vs. 분야별(의료, 출입국, 본인인증, 범죄 등)로 나눌 것인가? 아니면 다른 구분?

제1감으로 보자면 수집, 처리(보관), 활용, 보호 등의 단계로 나누는 것이 서술하기 쉽게 느껴질 수도 있겠습니다만, 생체정보의 정의를 어떻게 내리느냐에 따라서 달라질 수 있다고 봅니다. 다분히 의료적인 방법을 통하여만 얻을 수 있는 정보를 생체정보라고 한다면 위와 같은 단계적 구분이 쉽겠지만, 웨어러블 디바이스로 얻어지거나 얻어질 것으로 예상되는 정보까지 생체정보의 범주에 넣게 된다면 수집,

처리, 활용이라는 단계적 구분이 쉽지 않게 될 것입니다. (위치정보법이 처음에 소수의 수집자를 상정하고 만들었는데 스마트폰을 통하여 수집이 매우 쉬워지면서 현실과 괴리된 법제로 뒤쳐진 예를 생각하면 됩니다.)

2. “생체정보”의 의의

- 생체정보의 개념은? (연구계획서 5페이지의 ■ 기타 참고사항 참고)
- 기존 “개인정보” 등과의 차이, 구별실익은?
- 생체정보의 개념을 어떻게 보느냐(정의 내지 범위)에 따라 본 연구의 목적이나 방향이 많이 달라지게 되는지?

기본적으로 생체정보는 개인정보의 부분집합이 될 것입니다. 따라서 개인정보보호의 법리가 그대로 적용될 것이라고 생각합니다. 다만 생체정보의 개념을 특별히 정하는 것은 수집방법, 활용영역, 보호의 필요성이 일반적인 개인정보에 비하여 차이가 있기 때문일 것입니다. 따라서 생체정보를 어떻게 정의하느냐는 어떤 영역을 규율할 것이며, 어떻게 보호하고, 어떻게 활용할 수 있도록 할 것이냐에 대한 전체적 방향성과 밀접하게 연결되어 있다고 생각합니다.

특히 일반적 개인정보와의 개념차이 보다는 의료정보와의 구별이 중요한 포인트라고 생각합니다. 의료적 방법을 통하여만 얻을 수 있는 정보를 생체정보라고 한다면 전체적으로 서술이 어렵지 않을 것으로 예상되며, 웨어러블 디바이스를 통하여 수집될 수 있는 정보를 포함하게 된다면 연구의 영역이 상당히 넓어질 수밖에 없을 것입니다.

의견 6

정 소 영
(충북대 법학과 강사)

I. 연구의 방향과 범위

□ 생체정보의 활용과 보호

- 생체정보의 활용은 거스를 수 없는 대세로 보임. 2016.3.3. 국회입법조사처에서도 “스마트 시대의 생체정보 보호를 위한 입법과제”라는 글에서 생체 정보에 관한 입법적 개선을 촉구한 바 있어 매우 시의적절한 연구과제로 생각됨.
- 활용과 함께 보호 방안도 논하지 않을 수 없음.
- 개인정보보호법도 제1조 목적에서 “개인정보의 처리 및 보호에 관한 사항을 정함으로써” 라고 하고 있어 개인정보의 수집, 이용, 제공과 함께 보호에 관한 사항도 함께 규정하고 있음.

□ 보고서 체재 (주기별 혹은 분야별)

- 현재 생체정보는 주로 의료, 출입국관리, 본인인증, 범죄수사 등에 이용되고 있음. 각 분야별로 수집, 활용, 보호에 대한 검토가 모두 필요함. 즉, 종으로 분야를 나누고 횡으로 주기를 나눈다면 종적, 횡적 어느 방향으로의 검토도 가능함.
- 궁극적으로 어떤 결론을 제시할 것인가에 따라 보고서 체재도 결정되어야 한다고 생각됨. 개별 법령의 개정안을 제시하는 결론이면 분야별로 검토하는 것이 더 적합할 것이고, 생체정보에 관한 사항을 아우르는 새로운 제정법안의 입법을 제시하는 결론이면 주기별 검토도 가능할 것임.

II. 생체정보의 의의

□ 생체정보의 특성

- 미래사회를 잘 그려냈다는 평가를 받는 영화 <마이너리티리포트>에는 건물에 출입허가를 받기 위해 홍채인식을 하는 장면이 나옴. 주인공은 건물에 몰래 잠입하기 위해 이미 알려져 있는 자신의 홍채정보를 바꾸고자 함. 그러나 홍채정보를 바꾸고자 한다는 것은 어느 정도 반사회적, 혹은 범죄적 목적을 가진 것으로 취급되기 때문에 일반 병원에서는 시술하지 않음. 따라서 주인공이 뒷골목의 무허가 의사에게 눈수술을 받는 장면이 나옴.
- 생체정보의 가장 특별한 성질은 ‘불변성’이고 ‘고유성’이라고 생각됨.(그 외 우리 모두는 생체정보를 가지고 있다는 점에서 보편성이라는 특성도 있음) 즉 우리가 타고난 홍채정보, 망막정보, 정맥정보, 지문정보 등을 바꾸기는 매우 어려우며, 이러한 정보들은 개인마다 고유하게 가지는 것이기 때문에 한번 등록되면 그 등록정보는 평생토록 개인을 식별하는 데 사용될 수 있음.
- 변경하거나 폐기하고 새롭게 생성할 수 없으므로 생체정보가 오남용 되었을 때의 과급효과는 지금까지의 개인정보 오남용과는 비교할 수 없을 정도로 심각한 문제를 야기할 수 있음.

□ 생체정보 이용 목적의 다양성

- 아래와 같은 부처들로 생체정보에 관한 관할이 따로 이루어지고 있음
 - 미래창조과학부와 그 소속기관 직제 시행규칙 8. 생체 기반 인증 체계 관련 정책·제도의 수립·시행
 - 법무부와 그 소속기관 직제 시행규칙 3. 생체인식기술 등 국내외 첨단기술을 응용한 출입국·체류심사제도의 연구·개선

- 산업통상자원부와 그 소속기관 직제 시행규칙 5. 바이오(생체)인식 관련 기술개발 및 산업화에 관한 사항
- 그 외 해양수산부(선원법), 금융위원회(전자금융거래법), 미래창조과학부(전자서명법) 등
- 각 부처들이 생체정보를 통해 추구하는 바가 다를 것이므로 이러한 다양한 논점들을 포괄할 수 있는 연구 성과가 도출되었으면 하는 바램임.
- 생체정보는 현행 법제 하에서는 개인정보에 포함되며, 불변성과 고유성의 특징 때문에 민감정보에 해당할 가능성도 많음.

Ⅲ. 디스토피아적 결과의 방지

□ 아직까지는 생체정보 활용에 대한 두려움이 더 큰 것으로 보임

- ~정보는 제공하는 사람보다는 정보를 쥐고 있는 사람에게 유용한 것. 정보를 수집하려는 쪽에서는 더 많은 정보를 원하지만, 수집당하는 입장에서는 더 많은 정보를 제공하는 것이 더 큰 편리와 이익을 가져올 것인지는 불확실.
- ~최근 개인정보 이용의 활성화가 논의되고 있지만¹⁾ 활용은 주로 비식별정보에 국한되어 논의되고 있음. 식별정보에 대한 활용에 대해서는 아직까지 우려와 반감이 많은 상황. 그러나 생체정보는 ‘식별정보’ 중에서도 가장 근본적인 식별정보이므로 이에 대한 활용은 조심스럽게 접근해야 할 것으로 보임.
- 9.11 테러 이후 미국에서 생체정보가 담긴 전자여권을 보편화한 것이나, 현재 범죄수사에 생체정보가 활용되고 있는 것을 보더라도 생체정보의 수집과 활용은 개인적 편리성보다는 국가기관의 편리성을 담보하는 경향이 있음.

1) 세계일보 3월 17일 보도 “비식별정보 활용해야 빅데이터 산업 발전”

□ 결국 중요한 것은 정보 주체의 결정권 보장

- 분명히 내가 정보 제공에 동의한 적이 없는 것 같은데, 판촉전화나 여론조사 전화를 받으면 ‘이 사람들이 내 전화번호를 어떻게 알았을까’ 라는 의문이 들고 ‘전화번호를 알면 주소나 주민번호 등 다른 정보도 아는 것 아닐까’라는 불안이 들게 됨
- 정보의 수집과 제공, 유통 등에 정보 주체의 결정권을 실질적으로 보장하는 것이 인간의 존엄과 자유를 지키는 길이라고 생각됨(프라이버시권도 나 자신에 대한 공개/비공개를 스스로 결정할 수 있는냐의 문제)

제2차 워크숍
생체정보의 활용 현황에
관한 검토
- 바이오인식 분야 -

2016. 4. 29.

일 정

1. 목 적 : 생체정보의 활용 현황에 관한 검토회의 - 바이오인식 분야
2. 일 시 : 2016년 4월 29일(금) 12:00~18:00
3. 장 소 : 서울역 AREX-1 회의실
4. 세부일정
 - (1) 사회
 - 권건보(아주대 법학전문대학원 교수)
 - (2) 연구개요 발표
 - 김현희(연구책임, 한국법제연구원 연구위원)
 - (3) 발제
 - 이승재(한국인터넷진흥원 수석연구원)
 - 전동훈(SUPREMA 팀장)
 - 김건우(한국전자통신연구원 실장)
 - (4) 토론
 - 정필운(교원대 일반사회교육과 교수)
 - 유지연(상명대 지식보안경영학과 교수)
 - 방동희(부산대 법전원 교수)
 - 손형섭(경성대 법학과 교수)
 - 김현경(서울과기대 IT정책전문대학원 교수)
 - 정소영(충북대 법학과 강사)
 - 황현영(국회 입법조사처 법제사법팀)

목 차

□ 발 제 문	53
○ 생체인증(바이오인식 인증)을 이용한 인증기술 및 시장현황 (이승재)	55
○ 생체정보의 활용 현황 - 바이오인식기술(전동훈)	69
○ 바이오인식 기술의 발전 및 침해 요소(김건우)	83
□ 토 론 문	87
○ 토 론 문 1(정필운)	89
○ 토 론 문 2(방동희)	95
○ 토 론 문 3(정소영)	97
○ 토 론 문 4(황현영)	101

발 제 문

생체인증(바이오인식 인증)을 이용한 인증기술 및 시장현황

이 승 재
(한국인터넷진흥원 수석연구원)

생체인증(바이오인식 인증)을 이용한
인증기술 및 시장현황

2016. 4

KISA 한국인터넷진흥원
K-NBTC Korea National Biometric Test Center

0. 바이오인식 vs 생체인식

바이오인식

- 약 2009년부터 사용
- IT 표준에 많이 사용
- 법률에서 유사하게 사용
(법들 : 바이오 정보)
- 정부(미래부) 계획안에서 사용

생체인식

- 언론에서 사용
- 초기(2002년~2008년)에
많이 사용

목 차

- I 바이오인식 기술의 정의 및 종류
- II 바이오인식 제품 시장현황
- III 바이오인식 관련 법률 현황
- IV 바이오인식 인증 현황 및 전망

2

- I 바이오인식 기술의 정의 및 종류

3

1. 바이오인식 정의

바이오인식이란?
 사람의 신체적(얼굴/홍채/지문/정맥 등), 행동적(음성/사인/자판/걸음걸이 등) 특징을 자동화된 IT 기술로 추출·저장해, 다양한 IT 기기로 개인의 신원을 확인하는 수단

신체적 특징

- ② 얼굴
- ③ 홍채
- ④ 지문
- ④ 정맥
[손가락정맥] [손등정맥]

행동적 특징

- [음성]
- [사인]
- [자판입력]
- [걸음걸이]

4

1. 바이오인식 정의

바이오인 **바이오인식,**
 사람의 신 **몸으로 나를 증명한다.** 특징을
 자동화된 IT 기술로 추출·저장해, 다양한 IT 기기로 개인의 신원을 확인하는 수단
EBS, 원더풀사이언스 2008
YTN사이언스 특집다큐 2013

↓

**바이오인식이란,
내몸의 정보로
내가 나임을 증명하는 수단**

신체적 특징

- ② 얼굴
- ③ 홍채
- ④ 지문
- ④ 정맥
[손가락정맥] [손등정맥]

행동적 특징

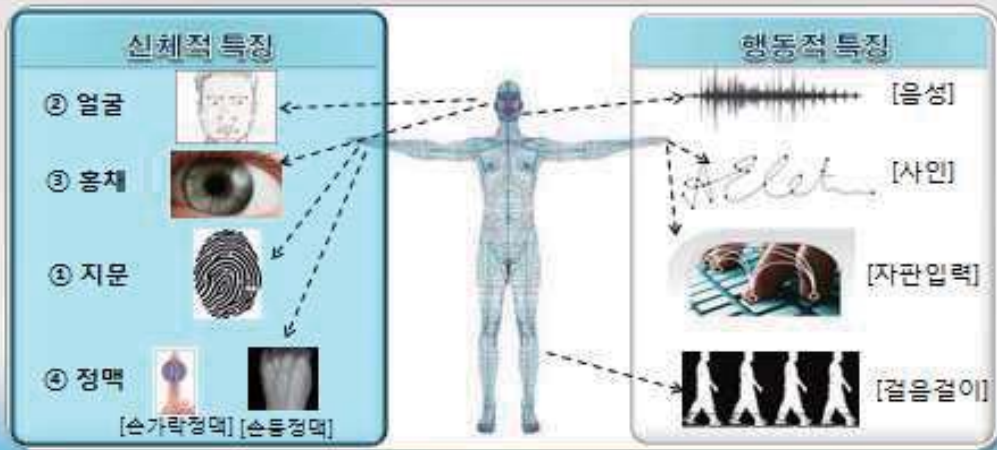
- [음성]
- [사인]
- [자판입력]
- [걸음걸이]

5

1. 바이오인식 정의

바이오인식이란?

사람의 신체적(얼굴/홍채/지문/정맥 등), 행동적(음성/사인/자판/걸음걸이 등) 특징을 자동화된 IT 기술로 추출·저장해, 다양한 IT 기기로 개인의 신원을 확인하는 수단



6

2. 바이오인식 종류별 장단점

④ 지문

- 가장 오래 사용된(100년 이상) 바이오인식 종류
- 임신 24주째에 생성되어, 평생 불변
- 무지문증, 다한증 등으로 약 2%정도는 지문 취득 불가



② 얼굴

- 얼굴 외곽, 눈/눈썹/코모양, 눈/코/턱 간격 등 측정
- 비접촉 방식으로 사용자의 거부감이 적음
- 환경(안경, 가발, 조명 등) 영향이 많고, 인식 시간이 오래 걸림



③ 홍채

- 홍채 모양, 색깔, 망막 모세혈관의 형태소 등 인식
- 생후 18개월에 모양이 완성된 후, 평생 불변
- 사용자 거부감이 높으며, 제품의 크기가 큼



④ 정맥

- 손등 또는 손가락의 혈관 형태를 측정
- 적외선 카메라를 이용, 혈관을 투시 후, 잔영을 인식
- 하드웨어 구성이 복잡해, 제품 가격이 고가임



7

3. 바이오인식 제품

바이오인식 제품은

바이오인식을 이용한 도어락, 무인민원발급기, 출입통제시스템 등의 제품이 있음



<지문 - 도어락>



<지문 - 무인민원발급기> <홍채 - 출입통제> <얼굴 - 출입통제> <정맥 - 출입통제>

4. 영화속의 바이오인식 및 제품

바이오인식 및 관련 제품은 액션/SF 영화에 자주 등장하는 소재로,
일반인에게 많이 알리는 계기가 되었으나, 사실과 다른 정보 전달이 있음

[007 다이아몬드는 영원히, 1971]

- 최초로 바이오인식(지문인식)을 영화에 등장시킴
- 지문(위조지문)으로 사람의 신원 파악

[마이내리티 리포트, 2002]


- 홍채를 이용한 다양한 바이오인식 제품 등장
- 단, 죽은 홍채를 이용한 바이오인식은 오류

(혈류, 망막, 움직임, 맥박 등 'Liveness'를 감지하는 센서
없거나 죽거나 위조된 바이오인식 정보는 감지가 않음)

5. 바이오인식의 중요성

사회적 가치로서의 중요성

- 2001년 911테러로 신원확인 수단으로 중요성 부각
- 미국/유럽 등 출입국 사무소에 바이오인식 제품 도입(04~05년)



산업적 가치로서의 중요성

- 미국, 유럽에 바이오인식 시험센터 설립, 운영
- 고성장 산업 (2~30%)
(물리보안 산업)
- 타 IT산업에 비해 고부가가치

10

[참고] 물리보안 산업 개요

물리보안산업이란, 정보보호(정보보안, 물리보안, 융합보안)의 한 분야로, 재난·재해, 범죄 등을 방지하기 위한 산업이며, CCTV 등 영상감시 및 저장장치, 바이오인식, 출입통제 관련 제품 및 서비스로 구성

<정보보호 산업>

정보보안	물리보안	융합보안
 <p>해킹/침입방지, 개인정보유출방지 컴퓨터바이러스 등 정보보안(물리인터넷경제)</p>	 <p>영상감시, 바이오인식, 주요전자감비 등 물리보안(안전안심생활)</p>	 <p>중소보안(자동차/항공 등) /의료/건설/국방 보안 합법보안제품 등 융합보안(안전성강화)</p>

11

II 바이오인식 제품 시장현황

12

1. 바이오인식 산업 국내외 시장 규모

전세계 94억달러 규모의 시장이며, 국내는 1.860억 매출을 기록('14년기준)

세계시장

- 지문인식이 전체시장의 66%이나, 얼굴인식과 홍채인식으로 확대 중
- 세계시장은 '11년 54억 달러 → '14년 94억 달러, 연평균 20% 성장



국내시장

- 국내 매출은 '13년 1,724억원 → '18년 4,147억원, 연평균 19.2% 성장
- 지문(989억), 얼굴(560억), 홍채(11억), 정맥(58억), 기타(100억) 차지('13년)



• 2014 국내 정보보호산업 실태조사(2014.12, KISA)

13

2. 바이오인식 산업 국내시장 세부내용

시장비율은 지문인식이 높으며(57%), 성장률은 홍채인식이 높을 것으로 예상

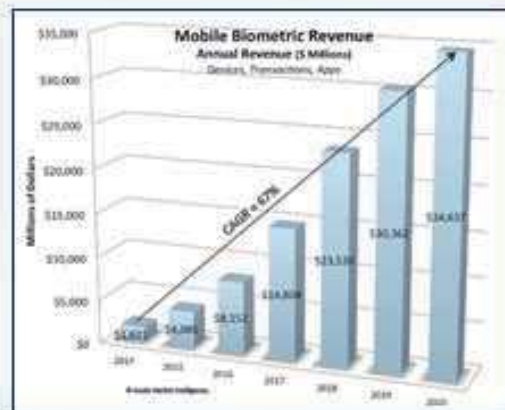
세부항목	2013년	2014년 (F)	2015년 (F)	2016년 (F)	2017년 (F)	2018년 (F)	CAGR (13~18)
얼굴인식시스템	56,086	59,619	84,577	111,627	147,328	194,447	28.2
지문인식시스템	98,983	107,840	128,002	139,455	151,933	165,528	10.8
홍채인식시스템	1,163	2,026	6,149	10,713	18,663	32,513	94.7
정맥인식시스템	5,863	6,601	7,346	8,199	9,151	10,213	11.7
기타음성인식 등	10,336	10,600	11,148	11,432	11,724	12,023	3.1
소계	172,431	186,686	237,222	281,426	338,799	414,724	19.2

14

3. 바이오인식을 이용한 스마트기기(모바일) 시장

연평균 67%씩 성장해 2020년에는 346억 달러(약 38.2조원) 시장 전망

- AMI는 스마트폰, 태블릿PC, 웨어러블 등 스마트 기기에 바이오인식 제품이 2020년 모두 탑재될 것으로 전망
- 2020년 까지 바이오인식 센서가 탑재된 모바일기기, 바이오인식 앱, 바이오인식 인증 시장 규모는 연평균 67%씩 성장해 346억 달러(약 38.2조원)에 이를 전망
- 바이오인식 센서가 탑재된 스마트기기는 2020년 100%에 이를 것이며, 바이오인식 앱은 2017년부터 시장 규모가 커지며, 바이오인식 인증은 결제 거래 및 사용자 인증 수단으로 이용될 전망



15

5. 출입통제시스템 (공공분야)

얼굴인식을 이용한 상주직원용 공항공사 출입통제시스템에 도입 확대

공항공사의 바이오인식 제품 도입 사례

- 전국 공항(15개)에 상주직원용 출입통제에 얼굴인식 시스템 도입
⇒ (현재) RF 카드로 출입통제 → (향후) RF 카드 + 얼굴인식
- 2013년 제주공항에 우선적으로 얼굴인식 시스템 도입 (향후 점차 확대)

제주공항 RF 카드 및 얼굴인식 시스템을 통한 출입통제 시스템 모습



- ① 출입구에 RF 태그 접촉
- ② 출입구 카메라를 통해 얼굴인식
- ③ 얼굴인식 성공시, 출입 가능

16

III 바이오인식 관련 법률 현황

17

1. 바이오인식 관련 법령

‘정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령’에 기술됨

• 2014년 11월 28일 개정

제 15조(개인정보의 보호조치)

④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자 등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호, 계좌정보 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장



개정전 시행령

1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장

18

2. 전자금융거래시 본인인증 관련 법령

‘전자금융감독규정’에 규정된 공인인증서 사용 의무 폐지

• 2015년 3월 18일

□ 공인인증서 등 사용 의무 폐지(제37조①~③항 개정)

• (내용) 전자금융거래시 ‘공인인증서 또는 이와 동등한 수준의 안전성이 인정되는 인증방법’을 사용할 의무를 폐지

• (효과) 다양한 전자금융거래 인증수단 등장·활용 유도



바이오인식, SMS, USIM, 기타(1회용 OTP 등)

19

3. 정보보호산업의 진흥에 관한 법령

정보보안, 물리보안(바이오인식 등) 진흥을 위한 법령 제정(2015.6), 시행(2015.12)

□ 수요측면: 정보보호시장 창출 등 산업 선순환생태계 강화

- 정보보호주자의 수요개발 및 시장 예측성에 기여하도록 하기 위하여, '공공기관 등의 구매수요 정보의 제공' 규정(제8조)
- 정보보호제품 및 서비스에 대해 재값을 주고 받을 수 있는 환경 조성 및 불합리한 발주 관행 개선을 위하여, '정보보호제품 및 서비스의 적정 대가'의 지급 노력 및 불공정 발주 관행 개선을 위한 '발주 모니터링 체계의 운영' 규정(제10조)
- 기업의 자발적인 정보보호 주자를 유도하기 위하여 '정보보호준비도 평가' 및 '정보보호금시' 제도 시행 근거를 마련(제12조, 제13조)

20

3. 정보보호산업의 진흥에 관한 법령

□ 공급측면: 체계적인 정보보호산업 진흥 기반 조성

- 정보보호산업 진흥의 기반 조성을 강화하기 위하여 범국가적 정보보호산업의 진흥에 필요한 정책 수립 및 예산을 확보하도록 하는 '국가 및 지방자치단체의 책무' 등 규정(제3조)하고 '정보보호산업 진흥 계획의 수립' 하도록 규정(제5조)
- 우수한 정보보호제품이 공급되도록 함으로써 정보보호기업 및 제품의 글로벌 경쟁력 확보를 위하여 '국제협력 추진' (제16조) 및 '성능평가 지원' (제17조) 및 '우수정보보호기술등의 지정' (제18조)과 '우수정보보호기업의 지정' 규정(제19조)
- 기술개발 및 인력양성을 체계적으로 할 수 있도록 하기 위하여 '기술개발 및 표준화추진' (제14조), '인력양성' (제15조), '정보보호산업의 융합추진' (제11조) 규정

21

IV 바이오인식 인증 현황 및 전망

22

1. 금융 거래시 개인인증

해외는 금융 거래시 바이오인식을 통해 본인을 인증하고 있으며, 국내도 바이오인식 등 핀테크 기술이 금융 거래에 적용될 것으로 예상

- 해외 사례
 - (미국) US Bank에 모바일 뱅킹서비스에서 개인정보 입력 없이, 목소리만으로 본인 확인 및 이체 가능
 - (영국) 바클레이는 손가락 정맥 인증을 통해 온라인 뱅킹 접속 등이 가능하도록 서비스 운영 중
 - (일본) Japan Post Bank, Maga Bank 등은 ATM내 정맥인식을 탑재하여 사용자를 인증
 - (기타) 터키, 인도, 호주 등 모바일 웹, ATM에서 지문, 음성, 홍채인식 등을 통해 사용자 인증

23

2. 전자결제시 개인인증

온라인 전자결제에 지문인식, 얼굴인식 등 도입 예정

• 사례

- 애플페이, 삼성페이 : 지문인식
- 알리페이 : 얼굴인식(예정)

< 알리바바 마윈 회장 얼굴인식 시연모습 >
(2015. 3월, 독일 하노버 세빛 2015)



24

3. 공인인증서 개인인증

공인인증서에 개인을 인증하는 수단으로 바이오인식 사용

• 사례

- 국내 KISA에서 공인인증서 이용시 지문인식으로 본인인증
- 그외 타 바이오인식 기술 도입 예정

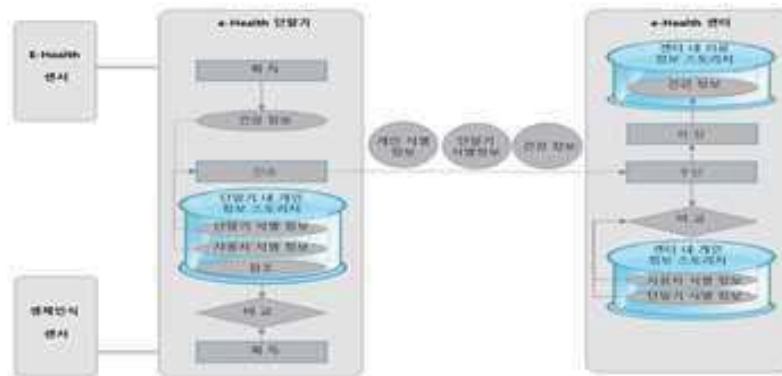
비밀번호 없는 공인인증서 이용 절차



25

4. e-Health에 환자 개인인증

원격진료/응급진료시 환자 개인인증을 위해 바이오인식 정보 사용
ITU-T 표준으로 e-Health에 개인인증 프레임워크 제정 중



26

[참고] 해외(미국) 바이오인식 인증 제도

미국 NIST에서 시험/평가하고, FBI에서 인증하는 PIV 제도 운영 중

- PIV(Personal Identification Verification) 인증제도
 - 바이오인식 제품의 성능 평가(미국 NIST) 및 인증(미국 FBI)하며, 미국 정부·공공기관에 바이오인식 제품 납품시 PIV 인증 필수

구분	인증/평가기관	인증내용	인증대상	근거	의무/가산 제도
PIV인증 (Personal Identification Verification)	<ul style="list-style-type: none"> ○ 인증 : 미국 FBI ○ 평가 : 미국 NIST 	<ul style="list-style-type: none"> ○ PIV 바이오인식 성능 인증 - 바이오인식 소프트웨어의 기능·신뢰·호환성 등 성능평가 	바이오인식 제품	미국 연방 컴퓨터리 규정 201조	미국 정부·공공기관에 바이오인식 납품시 PIV인증 의무화

27

생체정보의 활용 현황 - 바이오인식기술

전 동 훈
(SUPREMA 팀장)

[바이오인식 기술 종류 및 소개]

대표적으로 사용되는 바이오정보는 지문이다. 지문으로 신원을 인식하기 위한 연구는 1800년대 중반부터 시작되었고 1900년 이후에는 범죄자를 검거하기 위한 증거로써 본격적으로 이용되게 되었다. 이후 지문과 같이 신체의 유일한 부분을 이용해 신원을 확인하는 방법에 대한 연구가 계속 진행된 결과 현재는 홍채인식, 정맥인식, 음성인식 등의 신체적인 특성을 이용한 인증과 서명, 키 스트로크 등 행동적인 특성을 이용한 인증도 가능해지게 되었다.

<표 1> 바이오인식기술의 장단점 비교

바이오인식기술	장점	단점
지문(Fingerprinting)	비용 저렴, 우수한 안정성	지문이 보이지 않거나 손상될 가능성
얼굴(Face)	쉽고, 빠르고, 비용 저렴 편리하고 거부감 적음	조명 및 자세에 따라 영향을 받고 정확도 낮음
장문/손모양 (Palm/Hand Geometry)	최소의 저장용량 요구	처리속도가 늦고 정확도 떨어짐
정맥(Vein)	지문/손가락이 없어도 이용가능	시스템 소형화가 어려움
홍채(Iris)	기계와의 접촉이 불필요하여 거부감 적음	대용량 특징 벡터(256bytes)

바이오인식기술	장점	단점
망막(Retina)	안정성 우수	사용거부감
성문(Voiceprint)	비용 저렴, 원격접근에 적당	처리속도, 사람 상태에 쉽게 영향
필체(Signature)	비용 저렴	사람 상태에 쉽게 영향 높은 오인식률

출처: 중앙일보 ‘지문·얼굴·홍채·정맥.. 진화하는 IT 생체인식 기술, 2013년 12월 9일

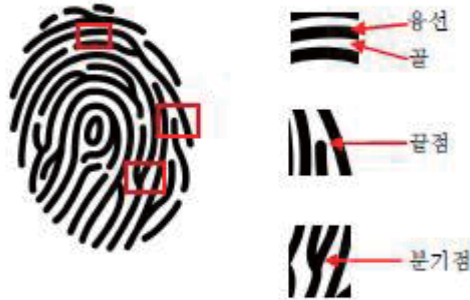
[신체적 특성 기반 바이오인식 기술]

바이오인식 기술 중 신체적 특성인 바이오정보를 이용한 기술은 지문 인식, 얼굴인식, 홍채인식, 화자(음성)인식, 정맥인식, 손모양인식, 장문(손바닥), 손바닥 혈관인식 등이 있으며, 이 중 두 개 이상의 기술을 동시에 이용하여 다중 바이오인식 시스템으로 응용하여 사용하기도 한다.

지문인식

1800년대 중반 영국의 William Herschel은 당시 영국의 식민지였던 인도에 일하던 세관원으로, 주변 사람들의 지문을 관찰하던 중 지문의 모양은 매우 다양하고 시간이 지나도 변하지 않는다는 사실을 깨닫게 되었다. 이후 영국 정부에서는 1877년부터 지문을 신원 인식의 방법으로 이용하기 시작하였다. 인증을 위해 사용되는 지문의 형태적인 특징은 그림과 같이 나타난다.

[그림 1] 지문의 형태적인 특징



지문에서 나타나는 여러 가지 형태의 선 모양을 융선, 융선과 융선 사이의 빈 부분을 골이라 하며, 융선의 흐름에 따라 생기는 분기점과 끝점이 존재한다. 지문을 이용한 인증을 위해서는 이러한 특징점의 모양과 위치를 이용하여 사용자의 고유한 템플릿을 만들고, 인증 수행 시 입력받은 데이터와 비교함으로써 인증을 수행하게 된다.

이러한 지문인식 방식은 기존의 인증방식에 비해서 분실, 망각할 가능성이 없고, 현재 가장 널리 사용되고 있는 생체인증기술로 도입이 쉽다. 하지만 지문을 이용할 수 없는 사용자들이 존재하기 때문에 이를 해결하기 위한 별도의 인증이 더 필요할 수 있다.

얼굴인식

모양 등의 얼굴의 특성을 이용하여 사람의 신원을 인식하는 방법이다. 그리고 얼굴의 특성을 이용하는 방법 외에도 열화상카메라를 이용하여 사람 얼굴의 고유한 열분포 패턴을 촬영하고 이를 이용하여 인증하는 방식도 존재한다.

지문인식 등 여타 다른 바이오인식 기술들보다 취득되는 영상에 영향을 미치는 환경적 요소가 매우 다양하여 취득된 영상을 비슷한 형태로 변환하는 전처리 과정에 많은 자원과 시간이 소모되는 특징이 있다.

또한 얼굴인식은 같은 인물이라 할지라도 주변 환경과 표정, 헤어스타일, 화장, 조명 등에 따라서 특징점의 변화가 비교적 크고, 전체적인 얼굴의 구성이 비슷한 사람들이 많이 존재하기 때문에 인식 정확도가 떨어지나 바이오정보 취득 장치에 직접 손가락이나 눈 등을 가까이 접근시켜야 하는 다른 바이오인식기술에 비해 영상 취득과정이 매우 간편하고, 기술의 발달로 처리속도 역시 계속 빨라지고 있어 앞으로 관련 기술에 대한 발전과 함께 얼굴인식기술 적용에 대한 관심 역시 점점 높아질 것으로 보인다.

홍채인식

개인마다 서로 구분되는 고유한 특징인 홍채패턴을 인식하는 기술이다. 사람의 홍채는 생후 18개월 이후 완성된 뒤, 평생 변하지 않는 특성을 지니고 있다. 또한 13만 가지 이상의 패턴 정보가 존재하며, 지문과 달리 홍채는 민감한 신체 부위로 눈꺼풀과 각막에 의해 다중으로 보호받기 때문에 손상으로 인한 변화 확률도 매우 희박하여 개인에 대한 유일성을 보장하는 데 뛰어난 바이오정보로 평가받고 있다.

홍채인식의 일반적인 과정은 먼저 일정한 거리에서 홍채인식기 중앙에 있는 거울에 사용자의 눈이 맞춰지면, 적외선을 이용한 카메라가 줌렌즈를 통해 초점을 조절한다.

이어 홍채 카메라가 사용자의 홍채를 사진으로 영상화한 뒤, 홍채인식 알고리즘이 홍채의 명암 패턴을 영역별로 분석해 개인 고유의 홍채 코드를 생성한다. 마지막으로 홍채 코드가 데이터베이스에 등록되는 것과 동시에 비교 검색이 이루어진다.

화자인식(음성인식)

음성으로부터 개인의 독특한 특성을 추출한 정보를 이용하는 인식을 화자인식이라고 하며, 다른 바이오인식에 비해 상황에 따라 에러

율은 높게 나타나지만 활발하게 연구되고 있는 분야이다. 음성 인식이란 사람이 말하는 음성 언어를 컴퓨터가 해석해 그 내용을 문자 데이터로 전환하는 처리를 말한다. 키보드 대신 문자를 입력하는 방식으로 주목을 받고 있으며 음성으로 기기제어, 정보검색이 필요한 경우에 응용되고 있다.

이러한 음성인식의 원리는 음성이 만들어 지는 과정과 밀접한 관계가 있다. 음성은 횡격막이 수축하면서 허파 속 공기가 밖으로 나오게 되는데 이때 성대와 성도를 지나면서 여러 가지 소리가 만들어 진다. 공기를 빠르게 보내면 압력이 더 낮아지고 성대들이 서로 부딪히는 속도는 빨라져 음의 높이가 높아지게 되는 것이다. 이후 성도를 지나면서 소리의 언어적 정보(발음)가 만들어지게 되는데 성도의 상태 즉, 입을 크게 벌렸는지 작게 벌렸는지, 혀끝이 윗잇몸에 붙었는지 아닌지와 같은 여러가지 상태에 따라서 다양한 소리가 나오게 된다.

화자인식은 다른 바이오인식 분야와 달리 원격지에서도 전화를 이용하여 신분을 확인할 수 있고, 별도의 교육이 필요하지 않다는 장점을 가지고 있지만 감기나 기타요인에 의해 목소리가 잠겼을 때, 타인의 목소리를 흉내내거나 주위환경에 소음이 있을 경우 취약하므로 보안분야에 적용하기 위해서는 잡음을 제거하는 기술이 선행되어야 할 것이다.

정맥인식

정맥 인식은 사람마다 손바닥, 손등 등의 혈관 패턴을 이용해 신분을 확인하는 인식 기법이다. 초기에는 가시광선 대역에 가까운 근적외선을 주로 사용하였으나, 지금은 적외선 영상을 이용해 혈관 모양을 열 형태로 읽어 들여 정밀도를 높인 제2세대 정맥인식 시스템까지 나와 있다.

정맥인식은 지문이나 손바닥의 손금을 이용하는 인식 기법보다 사용자의 거부감이 적고, 지문이나 손가락이 없는 사람도 이용할 수 있

다. 또 다른 바이오정보와 달리 정맥은 겉으로 드러나 있지 않고 피하조직에 존재하므로 복제가 어려워 높은 보안성을 가지고 있다. 반면 하드웨어 구성이 복잡한 특징이 있다.

손모양인식

지문인식이나 홍채인식과 같이 사용자가 지닌 신체의 물리적 특징을 이용하는 인식기법으로, 사용자가 인증을 위하여 기기상에 올려놓은 손의 모양에 대하여 상대적인 거리와 각도 등을 측정하여 기 저장해놓은 자신의 바이오정보와 비교하여 인증을 수행하는 방법임. 1980년대 초에 연구가 시작되었으며, 인증에서 높은 신뢰성을 제공한다는 장점으로 인하여, 제한된 사용자를 가진 인증 시스템으로 구축되고 있다.

[행동학적 특성 기반 바이오인식 기술]

키 스트로크 인식

사용자가 특정한 문자열을 타이핑할 때의 속도나 타이밍의 경향을 이용하여 개인을 인식하는 방법으로, 대부분의 사람들은 개인만의 독특한 타이핑 습관으로 인하여 각자 고유한 키스트로크를 갖게 되는 것을 이용한 것이다.

다른 생체 기반 정보의 경우, 인증에 사용되기 위해서는 추가적인 하드웨어의 설치가 필수적인 반면에, 키 스트로크 다이나믹스는 소프트웨어만으로 개인의 생체 기반 정보를 처리할 수 있는 장점으로 인하여 웹 기반 서비스의 대표적인 인증 방법으로 널리 연구되고 있다. 하지만 사용편의상 상대적으로 짧은 길이의 문자열에 대한 키스트로크만을 사용함으로써 제 3자의 인증 성공 가능성이 존재하고, 최초 인증 시 정상 사용자가 인증을 했으나, 중간에 세션을 탈취하여 해당 사용자의 권한을 사용하는 경우를 조기에 탐지하는 방법이 필요하다.

서명인식

서명인식이란 테플릿 또는 디지털라이저 등의 입력장치와 전자펜, 마우스 등을 이용하여 사용자가 기호나 서명을 실시간으로 시스템에 입력하여 등록된 기준서명과 비교하여 서명을 구별해 개인을 인식하는 기술이다. 서명은 약 1세기 전부터 계약 체결 등의 서류에 대한 증빙 목적으로 이용되기 시작하면서 법적인 효력을 얻음과 동시에 은행을 중심으로 널리 확산된 기술이다.

서명인식 기술에는 입력이 완료된 서명의 모양, 획 수, 각도 등을 인식하여 인증하는 정적인 방식과 사용자가 서명을 하는 실시간 과정을 동적으로 파악하여 서명을 쓰는 속도, 획 순서, 압력정보 등을 추출하여 인증하는 동적인 방식이 있다. 이중 동적인 방법이 보안 측면에서 더욱 우수하여 주로 사용된다.

걸음걸이 인식

사람은 원거리에서 다른 사람의 걸음걸이만 보아도 누구인지 구별해 내는 것이 가능하다. 모든 사람은 몸무게와 체형, 습관 등의 요인으로 인해 고유한 걸음걸이 패턴을 가질 수 있게 되고 이러한 행동적 특성을 이용하여 신원 확인을 하려는 시도가 바로 걸음걸이 인식(Gait Recognition) 기술이다. 출입통제 시스템에 걸음걸이 인식 기술이 적용되면 신원확인을 위해 멈춰 설 필요 없이 자연스러운 인증을 수행할 수 있어 사용자 편의성 면에서 매우 편리한 기술이다. 또한 다른 바이오인식 기술들에 비해서 위조하는 것이 매우 어려울 뿐만 아니라 얼굴인식 등의 기술과 달리 주변 환경에 크게 영향을 받지 않는다는 것도 걸음걸이 인식기술만의 장점으로 꼽을 수 있다.

[바이오인식기술 특징]

바이오인식기술에 사용되는 바이오정보는 각각의 바이오정보마다 고유의 특성이 있지만, 가장 중요하고 기본적인 특성으로 보편성, 고유성, 불변성을 만족해야만 한다.

보편성이란 바이오인식 시스템을 이용하는 모든 사람들이 인증하는데 사용되는 바이오정보를 지니고 있어야 함을 의미한다. 고유성은 시스템을 사용하는 사람들이 모두 구별되도록 사용되는 바이오정보가 사람들마다 각각 달라야함을 의미하고 영구성은 바이오정보가 시간, 조명과 같은 주변 환경에 따라 변하지 않는 특성이다.

바이오인식 기술을 적용하기 위해서는 응용 분야에 따라 적합한 바이오정보를 선택하여야 하며, 실제 응용 시스템에 적용하기 위해서는 정확도, 수용도, 기만용이도 등에 관한 고려가 있어야 한다.

성능(performance)이란, 목표로 하는 바이오인식시스템의 인식 성능, 계산속도, 하드웨어 자원 요구사항 등을 만족하는 바이오인식은 어떤 것인가를 고려하는 것을 말하며, 수용도(acceptability)는 일상생활에서 일반 사용자들이 받아들이기엔 거부감이 없는 바이오인식은 어떤 것인가를 말한다. 기만용이도(circumvention)는 잘못된 바이오정보를 이용하여 쉽게 시스템을 통과할 수 있는 바이오인식은 어떤 것인가를 고려한 것이다.

[바이오인식 기술의 표준화]

서로 다른 바이오인식 제품들의 상호호환성과 상호연동성을 고려한 기술 개발을 위해 표준화된 바이오인식 데이터와 API를 개발할 필요성과 바이오인식 제품들에 대한 성능 및 보안성 평가기술 개발의 필요성이 크게 증가하였다.

BioAPI

BioAPI는 컴팩이 1998년 4월 노벨, 마스터 카드, Microsoft, Miros를 포함한 후원자들과 함께 창설하였다. 2000년 3월 BioAPI 컨소시엄의 Version1.0이 공개되었고, 같은 해 9월 BioAPI Reference Implementation의 Beta Version이 공개되었다.

BioAPI는 multi-level로 개발되어 ‘상위-레벨’의 경우 등록, 인식 등을 제공하고, ‘하위-레벨’의 경우 세부적 제어, 정련, 기술적 의존도 등을 증가시키는 것에 주안점을 두고 있다. BioAPI는 단순한 어플리케이션 인터페이스 생성, 보안이 된 생체데이터 관리와 저장, 서로 다른 생체데이터와 디바이스 타입들의 표준 설치 방법 제안, 분산 컴퓨팅 환경에서 생체 인식을 제공하기 위한 목적으로 개발되었다.

X9.84

생체인증 데이터를 금융 분야에 적용하기 위한 노력의 하나로 데이터의 안전한 전송을 위해 ANSI의 X9소위원회 working group F4가 생체인증 데이터를 안전하게 주고받을 수 있는 데이터구조와 생체인증 데이터에 대한 최소 보안 요구사항을 표준으로 정의 한 것이 X9.84이다. X9.84에서 생체인증 데이터는 공개키(public key)를 통해서 무결성을 유지하고 조작된 생체인증 데이터로 부터 시스템 또는 개인정보를 보호하고 생체인증 데이터의 수집, 분산, 처리, 인증 등을 위한 보안 요구사항과 생체인증 데이터의 암호화, 전송 및 저장, life cycle, 프라이버시, 무결성 기술 등의 보안 요구사항이 있다.

CBEFF

생체인증시스템의 응용들 간의 Biometric data의 상호교환은 호환성 측면에서 매우 중요한 분야이며 제품개발 시 API와 더불어 범용성을 지원하기 위해서 필요하다.

Biometric data에 대한 초기 개념정의는 1999년 BioAPI Consortium과 X9.F4 working group에서 협의되어 2001년 3월 NIST ITL에서 CBEFF 명세를 발표 하였다. 이 명세에는 Biometric Header 및 data부분에 대한 명세를 지원하며, 생체자료 구조를 정의한 내용을 가지고 있다. 다양한 바이오인식 기술을 지원하기 위해 필요로 하는 공통된 데이터 요소들을 정의하고 있으며, 생체데이터 교환이 가능함에 따라 바이오인식기술을 기초로 한 응용프로그램과 시스템의 상호운용을 촉진하고자 하는 CBEFF는 하드웨어/소프트웨어 통합 처리의 단순화하고, 새로운 포맷이 어떻게 만들어질 수 있는지에 대해 설명하고 있다.

[바이오인식 기술 적용 분야]

바이오인식 기술의 경우 초기 출입관리 및 근태관리 등에 많이 적용되었으나, 기술에 대한 안전성이 높아지면서 금융, 보안 등 다양한 분야에서 활용되고 있다.

<표 2> 바이오인식 기술 적용 분야

구분	특징
금융	ATM-KIOSK, 모바일 뱅킹, 증권거래, 전자상거래, 지불 및 결제 수단 등
보안	정보보안(시스템 및 데이터 접근·인증제어), 생체로그인(PC용), 휴대폰/노트북/자동차 등 기기 사용자 인증 등
출입관리	공항(출입국 심사, 불법입출국자 확인 등), 기업(출입통제, 근태관리 등)
의료복지	환자 신분 확인, 기록 관리, 원격 진료, 무인전자처방전 등
공공	범죄자 인식(지문대조, 성문 분석 등), 전자주민증(신분증), 선거관리(본인확인) 등
마케팅	고객 연령 및 성별 추정, 타겟 마케팅(포인트 적립/이벤트 제공 등)

바이오 인식은 기술적으로 여러 명의 비교 대상 중 한 명을 알아내는 인식(identification)과 한 사람의 진위 여부를 판별하는 인증(verification)으로 나눌 수 있다.

인식 시스템은 템플릿 데이터베이스 전체를 검색하여 개인을 1 대 N으로 인식하는 것으로, 데이터베이스에 등록되어 있는 템플릿을 이용하여 누구인지를 판별하는 것을 말한다. 인증 시스템은 입력한 바이오 정보와 시스템에 미리 저장되어있는 템플릿과 비교하는 것에 의해 사람의 신분을 1 대 1로 인증하는 것으로, 신분이 제시한 권리를 판단하는 것을 말한다.

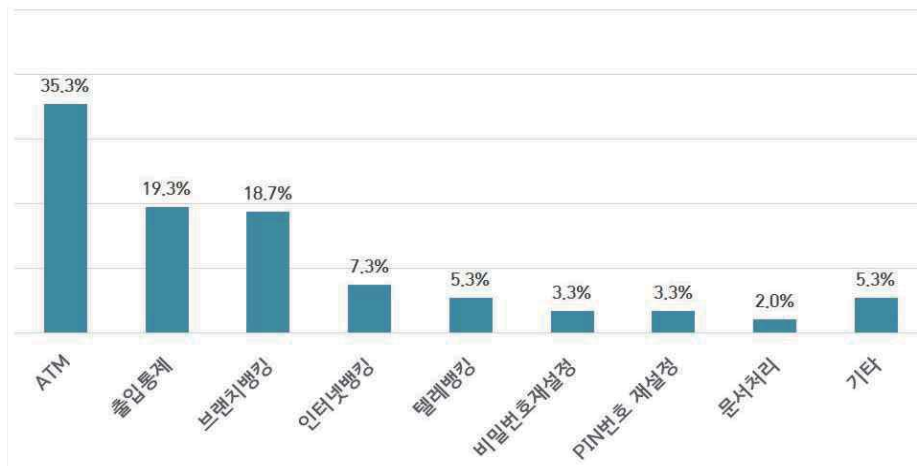
[금융기관에서의 바이오인증 적용현황]

금융거래는 크게 대면/비대면 방식의 거래로 구분할 수 있다. 대면거래란, 은행 창구에서 거래하는 것과 같이 사람이 직접 사용자의 인증

을 수행할 수 있는 경우를 의미하며, 비대면 방식은 텔레뱅킹, 인터넷뱅킹과 같이 직원과의 대면 없이 별도의 인증을 통해 거래를 진행하는 경우를 의미한다. 때문에 각 경우에 대한 인증 적용정도는 달라질 수밖에 없으며 일반적으로 비대면방식인 인터넷뱅킹, 폰뱅킹, ATM 거래 등에는 대면방식보다 강력한 보안 방식의 적용이 필요하다.

이러한 금융분야에서 바이오인식 기술을 가장 많이 이용한 사용처는 ATM으로 38%가량을 차지했고, 인터넷뱅킹과 Branch Banking이 그 뒤를 이어 각각 21%, 20%로 비슷한 비율을 보였다.

[그림 2] 사용 용도별 이용 비율



출처 Biometric Model for Iran's Banking System

금융기관에서 바이오인식 기술의 활용은 대표적으로 ‘본인인증’ 기능과 ‘지불결제’ 기능이다. ‘본인인증’ 기능은 전자상거래, ATM 사용, 금융사 지점에서 중요 거래시 본인 확인 등 다양한 금융관련 활동시, 당사자 본인임을 확인하는데 바이오인식 기술을 활용하여 기존의 보안 취약성을 대폭 보완할 수 있다. ‘지불결제’ 기능은 신용카드나 화폐 등 기존의 결제 수단에 의존하지 않고, 지문 등 바이오인식 기술의 활용만으로 지불 행위를 하여, 인증력과 고객의 편의성을 동시에 제고할 것으로 기대되고 있다.

<표 3> 국외 금융사기방지 바이오인증 도입 사례

도입 사례	적용 인식기술	시행 국가
자동화 기기 (ATM, VTM 등)	지문, 정맥, 홍채, 손모양 등	아, 노르웨이, 폴란드, 터키, 브라질, 멕시코, 콜롬비아, 인도, 요르단, 사우디아라비아, UAE, 나이지리아, 칠레, 브루나이, 남아프리카 공화국 등
바이오 인증 창구뱅킹	지문, 정맥, 얼굴, 음성, 서명 등	미국, 일본, 인도네시아, 폴란드, 멕시코, 파나마, 이스라엘, 이집트, 요르단, 레바논, 칠레, 남아프리카 공화국, 파키스탄 등
인터넷 뱅킹	지문, 홍채, 서명, 키스트로크 등	미국, 영국, 에스토니아, 푸에르토리코, 에콰도르, 예멘, 요르단 등
폰뱅킹	음성	미국, 영국, 중국, 호주, 네덜란드, 이스라엘, 브라질 등
모바일 뱅킹	모바일뱅킹 지문 (아이폰 Touch ID)	미국, 영국 호주, 네덜란드, 싱가포르, 터키, 남아프리카 공화국, 나이지리아 등

[민수에서의 바이오인증 적용현황]

기업 등에서의 출입통제와 근태관리를 위해 바이오인식 장비를 활용하는 경우가 현재 바이오인식 시장에서 가장 큰 비율을 차지하고 있다.

이 외 학원 출결관리, PC 로그인 등 개인 인증 분야에서 지문 등을 중심으로 다양한 바이오인식 기술이 적용되고 있다.

[공공기관에서의 바이오인증 적용현황]

경찰청에서는 지문정보를 기반으로 범죄 수사에 활용하고 있는 것은 전통적인 응용분야이다. 이 외 얼굴과 지문 정보를 기반으로 미아, 장애인 등 사회약자를 위한 대국민 서비스도 진행 중이다.

법무부의 경우 입국 외국인을 대상으로 얼굴과 지문 정보를 수집하여 출입국 외국인 관리를 진행하고 있으며, 외교부도 여권발급 시 본인 확인 용도로 경찰청과 협조 하에 지문 정보를 활용하고 있다.

행자부는 사전투표 등을 진행할 때나 인감증명서 등 주요 증명서 발급 시 본인확인을 위해 지문정보를 활용하고 있다.

바이오인식 기술의 발전 및 침해 요소

김 건 우
(한국전자통신연구원 실장)

바이오인식 기술의 발전 및 침해 요소

한국전자통신연구원

김 건 우

1. 바이오인식 기술 개요

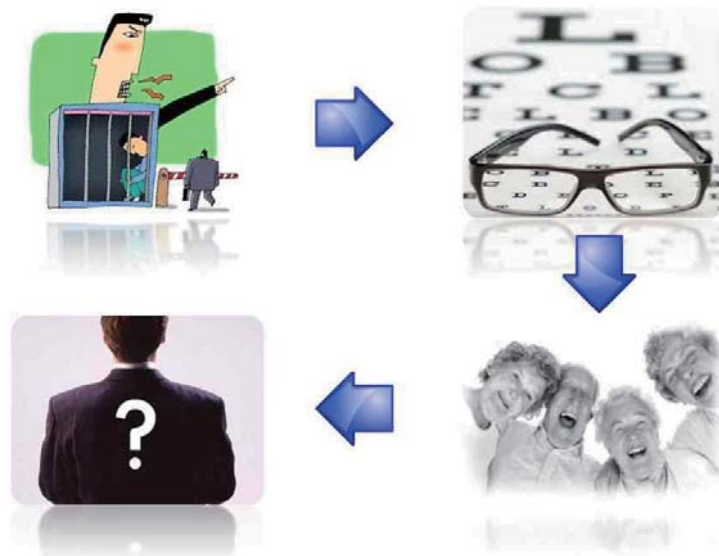
- 개 개인의 신체적·행동적 특징을 자동화된 장치로 추출·저장하여 정확하고 편리하게 개인의 신원을 확인하는 기술



II. 바이오인식 기술 종류



III. 발전 트렌드



Ⅳ . 기술별 현황



Ⅴ . 위험성 및 대응 기술

- 생체정보의 유출/분실 시, 이를 무효화하거나 다른 것으로 바꿀 수 없음
- 생체정보의 유출/분실 시, 책임기관을 알 수 없음
- 위조/인조 생체정보에 의한 오용



V I. 딜레마



V II. 결론



토 론 문

토 론 문 1

정 필 운

(교원대 일반사회교육과 교수)

1. 개념론(바이오인식, 바이오정보, 생체정보)

바이오인식(biometrics)

바이오, 통계

평생불변, 만인부동이라고 생각했기 때문에 인식 분야에 널리 쓰였다.

법률에서는 바이오정보라고 한다.

생체인식은 어감이 좋지 않다.

결론: 우리의 경우 생체정보라는 용어를 유지하여야 한다.

2. 유형론

생체정보의 두 가지 유형

(1) 신체적 특징

지문, 얼굴, 홍채(가장 성장률이 높을 것으로 예상, 위조방지로 보안
이 가장 뛰어나다. 정맥(비싼 것이 흠이다)

얼굴인식은 알리페이가 채용하겠다고 발표(마윈), 핸드폰에서 직접
구현할 수 있다는 장점이 있지만

생체인식: 적외선이 적혈구를 통과하지 못한다. 위조하기가 가장 어
렵다.

(2) 행동적 특징

사인, 자판입력, 걸음걸이, 입술움직임, in-air signature(3 발표자), 심박수(생체정보, 심박수를 통하여 자동차 여는 것)

- 음성은 신체적 특징이라고 하기도 하고, 행동적 특징이라고 한다.
- 걸음걸이는 디지털화해서 잘 안쓴다. 모방할 수 있게 때문에

결론: 이 두 가지 모두 생체정보라고 포섭하여 연구하여야 한다. (망법 시행령 제15조 제4항 제2호 바이오정보도 양자를 포괄하고 있다)

3. 응용분야

경향:

최초에는 범죄수사 등 부정적인 것, 밀착적인 것에 사용되었다. 현재에는 긍정적인 것, 비접촉인 것에 사용되었다.

앞으로 음성이나 얼굴인증이 많이 쓰일 것이다. 핸드폰 환경에서 사용자 친화적으로 인증할 것이다.

(1) 범죄수사에 가장 많이 쓰임

지문은 증거가 된다.

홍채는 아직 증거로 안된다.

(2) 출입통제, 근퇴관리

쓸 수 있는 것이냐.

(3) 금융에서 인증

핀테크와 연결하여 금융에서 인증업무에 많이 쓰려고 한다.

아직은 물음표

- 1) S은행에서 비대면계좌 개설에서 ATM에서 정맥정보를 쓰는 것.(VTM)

다른 두 은행에서 홍채 정보를 쓰겠다고

- 2) 텔레뱅킹

음성인식에 쓰겠다

- 3) 스마트폰의 쇼핑에서

마윈의 예. 얼굴 인식

(4) 이헬스에서 환자 개인인증:

긴급의료 때 환자 인증과 유용하다.

각 매체마다 장단점이 크게 나뉘기 때문에,
어떤 환경에서 어떻게 사용하느냐에 따라 다르다.

(5) 전자여권

여권발급 안되는 사람을 못하게 하는 것

(6) 행자부

초등학생, 치매환자 등에게 사전등록을 하도록 하고, 미아 발생시 바로 찾아 주고 있다. 부정적인 것이 아니라 긍정적인 것으로 사용되고 있다.

(7) 사전투표

사전투표시 본인인증을 위한 보조적인 수단으로 사용. 긍정적인 응용 분야

갤럭시 6에 홍채인식을 적용하는 것 검토하고 있다. IR센서를 달아야 하는데 비용이 많이 든다.

결론: 양대 분야(바이오인식과 이헬스), 그 밖의 응용서비스로 분류하여 서술

구글글라스로 경찰이 얼굴 인식하는 것을 허용할 것인지가 문제이다. (현행법으로는 불법일 것. 그런데 이것을 허용할 것인지)

페이스북에서 이용자 정보를 이용하여 딥러닝하는 것을 허용할 것인지 문제이다. (현행법으로는 불법일 것. 이런 것을 허용할 것인지)

이헬스-홍채에서 건강정보를 뽑아내어 전송, 저장하는 예, 당뇨병 관리를 위하여 생체정보 전송, 저장하는 예

4. 법제 현황 및 문제점

(1) 개인정보보호법

(2) 망법 시행령 제15조 제4항 제2호 바이오정보

바이오인식이라고 써야 한다.(1 발표자)

개정: 일방향이라는 것이 없어졌다.

이 개정으로 양방향도 포섭될 수 있다.

일방향: 받으면 줄 수 없다.

양방향: 주고 받는 것이 가능하다.

바이오를 이용해서 전자결재를 할 수 없다.

(3) ‘전자금융감독규정’ 제37조 제1항-제3항에 규정된 공인인증서
사용 의무 폐지

이제는 다양한 전자금융거래 인증수단 활용이 가능하다.

여태까지 2. 3. 규제 때문에 기술이 많이 발전하지 못하였다.
(기술중립성 원칙에 위배되었다. 이제라도 다행이다)

(4) 정보보안산업진흥법

계획. 올해 발표. 정보보안산업진흥을 위한 것들이

(5) 정보통신부 2005년 바이오정보보호 가이드라인 제정

2007년 단 한 차례 개정.

행자부에서 개정을 하려고 하고 있다.

딥러닝 기술을 이용한 얼굴 인식. 사람이 인지하는 것이 96.???% 라고
하는데, 이것이 97.?? 라고 한다. 즉 사람과 비슷한 인식율을 자랑한다.

얼마나 많은 학습데이터를 구축하여 러닝하는지가 문제. 페이스북이
가장 앞서고 있음. 그럴 수밖에 없음. EU가 이것을 문제삼고 있음.

(6) 문제점

유출시 무효화하거나 다른 것으로 바꿀 수 없다.- 그래서 사용을 못하
게 하는 것. 취급에 주의를 하도록 의무화(규범에 의한 대응). (새로운
대안) 폐턴화하여 사용하도록 하는 것(기술에 의한 대응)(김건우 실장님)

몇 개 기관에 주었을 때 유출한 책임기관을 알 수 없다.

위조 생체정보에 의한 오용

5. 진흥에 있어서 법적 문제

산업적 측면에서 진흥을 위하여 구체적인 법제 문제가 무엇인지?
(이승재 수석연구원님)

토 론 문 2

방 동 희
(부산대 법전원 교수)

생체정보의 활용 및 보호를 위한 법제 수립에 있어서 검토할 포인트는 다음과 같다고 여겨집니다.

- 생체정보의 정의
 - 현재 활용되고 있는 생체정보는 지문, 얼굴인식, 홍채, 정맥 등 임
 - 법제 설계에 있어서 가장 기본 - 출발 - 은 법제가 규율하려고 하는 대상임
 - 따라서 생체정보의 정의, 개념, 범위를 어떻게 하고, 어디까지 할 것인지가 매우 중요함
 - 법제를 통해서 규율체계 내로 수용하려는 것은 여러 의도가 있겠으나, 가장 기본적으로 해당 생체정보, 그 활용 등에 있어서의 위험성이므로 이를 감안하여 생체정보의 대상과 범위를 확정하여야 할 것임
- 생체정보의 생성 및 활용과 폐기의 생애주기별 규제 구조의 설계
 - 다음은 생체정보가 생성부터 활용되고 폐기에 이르는 실제 상황을 매우 상세하게 파악하여야 할 것임
 - 생체정보의 생애주기의 구체적 파악과 분석이 있는 이후에 각 단계별로 오용이나 남용의 위험, 또는 그 사용 또는 유통 자체가 위험한 부분 등 각종의 위험영역을 세부적으로 파악해야 할 것임
 - 각종의 위험의 영역이 구체적으로 파악되면 해당 위험을 관리 통제할 수 있는 규제의 유형을 선정 설계해야 할 것임

- 생체정보관리자에 대한 규제 설계의 검토
 - 상기 생체정보의 생성과 활용과 폐기의 생애주기별 규제 구조를 설계함에 있어 자연스럽게 생체정보관리자에 대한 규제가 설계되겠지만, 행위규제 이외에 상태를 규제, 또는 사업자 규제(입출입 등 진입규제, 지속적 관리규제) 해야 할 영역이 있다면, 이에 대한 규제설계를 해야할 것임
- 생체정보관리자에 대한 규제방법의 검토
 - 자율규제방식, 규제전담기구 등에 대한 규제방식과 방법 등 규제 수단에 대한 검토가 이뤄져야 할 것임
- 상기 규제 위반 및 불이행에 대한 제재 수단에 대한 검토
 - 앞단의 규제 형태와 내용이 도출되면 이에 대한 제재수단 등 행정의 실효성을 확보할 수 있는 방법을 강구해야할 것임
 - 행정벌, 행정질서벌, 이행강제금, 명단공표 등
- 생체정보 활용 진흥책에 대한 진흥책 검토
 - 표준제도 마련, 인센티브, 서비스이용활성화, 기금 마련 등에 대한 검토가 이뤄져야할 것임

토 론 문 3

정 소 영
(충북대 법학과 강사)

I. 용어사용의 문제

- 본 연구의 주제가 ‘생체정보’에 관한 것인데 생체정보를 어떻게 정의하느냐에 따라 연구의 범위가 달라질 수 있음
- 현재 법과 시행령, 가이드라인 등에서는 생체정보와 바이오정보가 둘 다 사용되고 있으며 통일적인 정의 규정은 없다고 보여짐
- 연구의 주제인 ‘생체정보’가 키와 몸무게 등 생체를 측정하여 얻을 수 있는 일반적인 모든 생체정보에 관한 것인지 아니면 생체에 기반해 개인을 인식할 수 있는 biometric정보에 관한 것인지를 결정하는 것이 필요함
- 사건으로는, ‘생체에 기반하여 개인을 인식하고 인증할 수 있는 정보의 활용과 보호’로 주제를 한정시키는 것이 좀 더 시의적절하고 활용가치가 있을 것으로 생각되며, 그럴 경우에는 생체정보라는 불명확한 용어보다는 ‘생체인식정보’ 혹은 ‘바이오인식정보(한국인터넷진흥원 사용 용어)’ 라는 용어를 연구보고서에서 사용하고 그에 따라 관련 법규정들의 통일적인 개정을 촉구하는 것이 적절하다고 생각됨.
- 오늘 발표하여 주신 발표자분들께서는 법학이 아닌 생체인식정보와 관련된 분야의 전문가들이신데 이 분들이 쓰시는 용어는 ‘바이오인식(biometric)’으로 통일되어 있었음.
- biometric을 생체인증으로 번역하는 예도 있으나, ‘인증’에는 인식하고 더 나아가 증명한다는 뜻이 포함되어 있으므로 인식에 중점

을 둘 것인지 증명하는 것까지를 포함할 것인지에 따라 용어를 선택하여야 한다고 생각됨.

II. 본인인증수단으로서의 생체정보 활용

□ 공공 영역에서의 활용

- 최근 행정자치부에서는 2018년에 공인인증서를 대체하는 본인확인 수단으로 모바일 생체인식 또는 IC카드인식 서비스를 제공하는 것을 목표로 하여, 지문·안면인식 또는 아이시(IC)칩 신분증 인식 방식으로 본인인증을 하는 방안에 대해 연구 중이라고 밝혔음
- 또한 행정자치부는 서울 정부청사 보안강화를 위해 국립과학수사 연구원이 개발한 얼굴인식시스템 시범운영을 시작하였고, 청사보안강화 태스크포스(T/F)팀은 얼굴인식, 홍채, 지문, 정맥 등 생체인증을 청사출입에 도입하기 위해 기술을 검증 중이라고 함.

□ 민간 영역에서의 활용

- 현재 사용자 인증 시 가장 많이 사용되는 방식은 아이디와 패스워드를 입력하는 방식임. 이 방식은 사용자들이 패스워드를 기억하기 쉽도록 하기 위해 간단하게 만들고, 가입 중인 여러 사이트에 동일한 아이디와 패스워드를 사용한다는 치명적인 보안 취약성이 있음.
- 이러한 문제점을 해결하기 위하여 바이오인식기술을 사용하여 사용자를 인증하는 파이도(FIDO, Fast Identity Online) 이 등장하였고, 온라인 환경에서 생체인식기술을 활용한 인증방식인 FIDO에 대한 기술표준을 정하기 위해 2012년FIDO Alliance가 설립되었고, 2014년 국제 인증기술 표준이 공개되었음
- 현재 출입관리 외의 생체 인증은 금융 서비스 분야에서 활용도가 높은 편임. 금융결제원이 2016년 5월에 생체정보 분산관리시스템

구축에 착수하였음. 생체정보 등록 템플릿 조각을 금융회사와 금융결제원이 분산 관리해 보안을 강화하는 방식을 취할 것으로 보도되고 있으며, FIDO인증기술 및 분산관리기술을 개별 금융회사에 지원할 계획이라고 함.

- 이와 같이 공공 영역과 민간 영역 모두에서 바이오인식에 기반한 본인 인증 시스템의 광범위한 활용이 눈 앞에 있는 것으로 보임.

Ⅲ. 법제도의 정비가 오히려 새로운 규제가 되지 않아야 함

- 바이오인식 기술을 보유한 국내 최대의 기업인 슈프리마의 전동훈 팀장님께서 발표 중에 말씀하시길, 슈프리마의 전체 매출의 70~80% 정도는 해외 수출에서 나온다고 하셨습니다.
- 바이오인식과 관련한 법제도의 정비가 오히려 새로운 규제를 만들어 내는 결과를 야기하지는 않아야 할 것임.
- 일례로 법학자들이 바이오인식 기술의 정확성과 보안 강화를 위해 ‘국제인증’을 도입하는 것이 어떠냐고 질문했을 때, 바이오인식은 계속 발전하고 있는 기술이기 때문에 국제인증같은 것이 별도로 정해져 있기가 힘들고 혹은 국제적 표준이 있다하더라도 우리나라의 영세한 기업들이 그 표준에 맞추고 인증을 받기는 어렵다는 업계의 현실을 잘 모르시는 말씀이라는 설명을 하셨습니다.
- 수출과 무역에 의존하는 바가 큰 우리나라의 경제 상황에서 자국민의 바이오인식 정보를 보호하려는 목적으로 우리나라 안에서의 규제를 강화하는 것이 자국민과는 상관없는 해외 수출까지 위축시키는 결과를 가져올 수도 있다는 생각이 들었음.

IV. 생체인증의 부인방지의 효력에 관한 법률적 문제점

- 부인방지란 해당 거래 당사자가 본인의 행위임을 부인할 수 있는 가능성, 즉 타인의 명의도용거래의 가능성을 방지하는 것.
- 바이오인식과 관련하여 바이오인식 정보의 도용이나 유출가능성이 주로 논의의 대상이 되고 있으나, 그 반대의 경우도 법적 문제점을 내포하고 있음.
- 현재 전자서명법에서는 공인인증서에 기초한 전자서명에만 부인방지의 추정효를 부여하고 있음. 따라서 공인인증서가 사용된 거래에 대하여는 자기가 한 것이 아니라고 주장하는 이용자가 도용사실을 증명해야 함
- 생체인증을 통한 거래는 반대로 금융회사가 이용자 본인의 행위였음을 증명해야 함. 타인 지문등록, 도덕적 해이(moral hazard)에 따른 명의자와 범죄자의 결탁 범죄를 막을 수 있는 입법적 논의도 필요할 것으로 보임.

토 론 문 4

황 현 영
(국회 입법조사처 법제사법팀)

I. 들어가며

지금까지는 개인의 지문, 얼굴, 홍채 등의 생체 정보를 사용하는 것이 프라이버시를 침해할 수 있다는 이유로 출입국관리시스템을 제외하고는 제한적으로 이용되었다.¹⁾ 그러나 최근에는 생체 정보 인식을 통해 본인을 인증하는 방식에 대한 관심도가 높아지고 있고, 기차역의 물품보관소에서도 지문인식을 통한 물품보관방식이 도입될 정도로 이러한 인증방식이 상용화 되어가고 있다. 생체 정보 인식을 통한 본인 인증은 이용하기 편리할 뿐 아니라 불가변적인 생체정보의 특성상 보다 확실한 본인 인증을 가능하게 한다는 장점이 있다. 그러나 한편으로는 생체 정보라는 개인의 정보를 어떻게 보호할 것인가 하는 문제와 생체 정보가 위조될 경우 이를 어떻게 식별할 것인가 하는 문제가 제기될 수 있다. 따라서 본인 인증차원에서 생체정보 활용의 장점을 감안하여 이를 활성화 하는 동시에, 개인정보 보호 및 위조 대책 마련 등을 함께 강구할 필요가 있다.

II. 본인 인증 차원에서 생체정보 활용의 장점

우리나라의 경우 주민등록번호가 전 국민에게 부여되고, 이를 통해 여권, 주민등록증 등 본인인증이 가능한 신분증이 발급되고 있다. 그런데 문제는 법원에 생년월일 정정을 청구하고 이를 통해 생년월일이 정

1) 신용녀, “해외 금융권 바이오인식 사례 및 표준화 동향”, 전자금융과 금융보안, 2015.7. 4면.

정될 경우, 이에 따라 주민번호도 달라지게 되고 신분증도 달리 발급되어 본인 인증의 오류가 발생할 수 있다는 점이다. 특히 최근에 생년월일을 늦추어서 정년을 연장하고 반대로 생년월일을 앞당겨서 연금수령일시를 앞당기고자 하는 목적으로, 법원에 생년월일 정정을 청구하는 사건이 늘고 있다. 이를 통해 생년월일이 정정될 경우 주민등록번호가 정정되고 이에 따라 새로운 신분을 부여받게 된다. 실제로 출국금지된 상황에서 주민번호 정정을 통해 여권을 새로 발급받아 출국한 범죄자에 대한 사례도 조사되었다. 가장 확실하다고 하는 주민등록번호를 통한 신분증 마저도 경우에 따라서는 확실한 본인 인증의 수단으로 기능하지 못한다는 문제가 있다. 그러나 지문과 홍채같은 생체정보는 외부적 요인에 의해 변하지 않는 특징을 가지고 있으므로 본인 인증을 위한 용도로 활용하기에 적절한 수단이 될 수 있다.

Ⅲ. 개인정보 보호 및 위조 대책 마련

생체 정보를 활용한 본인 인증 방식이 편리하고 확실하다는 장점이 있으나, 이러한 생체정보가 유출되었을 때 그만큼 위험성이 따르게 된다. 주민번호나 개인 계좌번호, 핸드폰 번호와 같은 개인 정보는 유출의 문제가 발생하면 이를 변경할 수 있는 여지가 있다. 그러나 지문과 홍채와 같은 생체정보는 유출이 발생하여도, 이를 변경하거나 정정할 수 없다는 문제가 있다. 더욱이 기차역 물품보관소 등과 같이 생체정보를 활용하여 본인 인증 하는 방식이 상업화 될 경우, 개인정보 보관 및 처리에 대해 적절한 통제를 하기도 어렵다. 금융기관이나 국가기관에서 이러한 생체 정보를 활용할 경우 이에 대한 감독이 비교적 용이하지만, 개별 사기업이 이를 활용할 경우 개인 정보를 제대로 보관하고 처리하는지 여부를 모두 점검하고 감독하는 것은 불가능하다고 해도 과언이 아니다. 또한 범죄 현장에서 지문의 발견은 중

요한 수사의 단서가 되므로, 만약 이러한 생체 정보가 유출되어 범죄에 이용된다면 지금까지 개인정보 유출과는 다른 양상의 문제가 발생할 수 있다. 따라서 생체 정보와 같은 민감한 개인정보를 보호하기 위한 방안과 함께 이를 위조하지 못하도록 하는 방안이 함께 검토될 필요가 있다.

제3차 워크숍
생체정보의 활용 현황에
관한 검토 (2)
- 금융, 의료, 범죄수사 분야 -

2016. 5. 27.

일 정

1. 목 적 : 생체정보 활용 현황에 관한 검토회의(2)
- 금융, 의료, 형사수사 분야 -
2. 일 시 : 2016년 5월 27일(금) 12:00~18:00
3. 장 소 : 서울역회의실 제1호
4. 세부일정
 - (1) 사 회
- 권건보(아주대 법학전문대학원 교수)
 - (2) 연구개요 발표
- 김현희(연구책임, 한국법제연구원 연구위원)
 - (3) 발 표
- 이창범(김장법률사무소 전문위원)
- 배현아(이대 생명의료법연구소 교수)
- 정소영(충남대 법학과 강사)
 - (4) 토 론
- 김종배(서울디지털대 컴퓨터공학과 교수)
- 문제선(OPA 전략사업팀장)
- 방동희(부산대 법전원 교수)
- 손형섭(경성대 법학과 교수)
- 오태원(경일대 법학과 교수)
- 유지연(상명대 지식보안경영학과 교수)
- 윤석진(강남대 법학과 교수)
- 정필운(교원대 일반사회교육과 교수)

목 차

□ 발 제 문	111
○ 생체정보의 분야별 활용현황 - 금융, 의료, 수사 분야(이창범)	113
○ 생체정보의 활용 및 보호를 위한 법제 정비방안 연구 : 생체정보의 분야별 활용현황-의료분야(배현아)	127
○ 생체정보의 분야별 활용현황 - 범죄수사 분야(정소영)	147
□ 토 론 문	163
○ 토 론 문(김종배)	165

발 제 문

생체정보의 분야별 활용현황 - 금융, 의료, 수사 분야

이 창 범
(김장 법률사무소 전문위원)

I. 금융분야

1) 최근동향

- 미국, 캐나다 등과 같이 신분확인제도가 발달하지 않은 나라에서 사회보장의 부정 수급을 방지하기 위한 신분확인 수단으로 이용되어 온 생체인식정보가 최근 ICT 기술과 융합하면서 민간영역에서도 새로운 인증수단으로 각광을 받고 있음
- 특히 2012년 온라인 환경에서 생체인식기술을 활용한 인증방식에 대한 기술표준을 정하기 위하여 FIDO 얼라이언스가 설립되면서 지문, 홍채, 안면윤곽 등의 생체정보를 이용한 인증방식에 대한 관심이 급증함
- 국내에서는 핀테크 열풍과 함께, 2015년 말부터 금융권의 비대면 금융거래가 허용되고 비대면 금융거래시 실지명의 확인수단의 하나로 생체인식이 포함되면서 공인인증서를 대체할 수단으로까지 평가받고 있음
- 그러나 생체정보의 활용에는 아직 많은 윤리적, 법률적 제약이 따르며, 기술수준도 고도화되어 있지 않아 생체정보의 활용을 어느 정도, 어느 방법으로까지 허용해야 할지에 대해서 검토해야 할 과제가 많음

2) 생체정보의 거래 및 활용 제한

- 생체정보는 지문, 홍채, 정맥, 얼굴윤곽, 유전자 등과 같이 살아있는 사람의 신체(생체)를 통해서 얻어지는 정보이므로, 연구 또는 기술개발의 목적이든 본인확인의 목적이든 생체정보를 거래의 대상으로 허용할 경우 윤리적 문제를 낳을 수 있음
 - ⇒ 생체정보는 법률에 의한 경우나 급박한 생명·신체·재산상의 이익을 보호하기 위한 경우가 아니면 원칙적으로 동의 받은 목적으로만 이용이 가능함
 - ⇒ 특히 정보주체의 사전 동의없이 생체정보를 통해 인종 식별, 건강상태 파악 등의 목적으로 이용해서는 안 되며, 생체정보를 차별적인 목적으로 활용해서도 안 됨
 - ⇒ 생체정보는 원칙적으로 거래의 대상이 되어서는 안됨. 다만, 생체정보를 연구목적으로 이용하고자 할 때에는 거래가 가능하나, 서면에 의한 명시적 동의에 의해야 함

3) 생체정보의 안전한 관리

- 생체정보는 생래적이고 일신전속적이어서 한번 유출되면 변경 또는 교체가 불가능함

<원본정보의 보호>

- ⇒ 원본정보를 저장하거나 송수신할 때에는 원본정보와 이름·주민번호 등의 식별자를 구분하여야 하고, 암호화되어야 함. 구분저장은 권장하나 필수적 요구사항은 아님.
- ⇒ 생체인식정보(특징정보)가 확보되면 원본정보는 원칙적으로 지체없이 파괴되어야 함

⇒ 연구목적, 생체인식정보의 재발급 등을 위해 원본정보를 보존하고자 하는 경우에는 특징정보의 수집.이용에 대한 동의와 구분하여 원본정보의 수집.이용에 대해서 정보주체의 명시적인 동의를 받아야 함

<특징정보의 보호>

⇒ 생체인식정보(특징정보)를 저장하거나 송수신할 때에는 이를 안전한 암호알고리즘으로 암호화 또는 일방향 암호화하여야 함.

4) 생체정보 활용의 장애요인

○ 국내 환경

- 금융실명제, 부동산실명제 등에 따라 관련법에서 사용자 인증보다는 실지명의 확인(실명확인)을 요구
- 법령상 실지명의 확인을 요구하지 않은 경우에도 거래계 전반에 걸쳐 사용자 인증보다 실명확인에 익숙

○ 사용자 인증

- 생체인증은 가장 완벽한(?) 사용자 인증(본인확인) 수단이지만, 그 자체만으로는 실지명의 확인 수단이 될 수 없음
- 주민등록시스템에 등록된 주민등록번호를 통해 확인된 실지명의와 반드시 결합되어야 실명확인수단으로서 효력 인정

○ 실지명의 확인

- 생체인증을 사용자 인증수단으로 이용하지 않고 실지명의 확인수단으로 이용하고자 할 때에는 주민등록번호와의 결합이 불가피함
- 정보통신망법상 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(대체수단)을 제공하고자 하는 자는 방송통신위원회로부터 본인확인기관으로 지정을 받아야 함

- 따라서 실지명의 확인을 위한 “생체인증서비스”를 제공하고자 하는 자도 본인확인기관으로 지정받아야 하는지 여부가 문제될 수 있음
 - 또한 생체인증서비스가 전자서명법상 공인전자서명으로 인정받기 위해서는 미래창조과학부장관으로부터 공인인증기관으로 지정을 받아야 함
- 생체인증이 아무리 뛰어난 인증수단이라도 우리나라 현실상 본인 확인수단 또는 공인전자서명으로 인정받지 않으면 한계가 있을 것으로 예상됨

II. 의료분야

1) 최근동향

- 유전자 분석은 암, 치매 등의 유전적 질환이나 난치병 또는 불치병의 예방 및 치료 등에 다양하게 이용될 수 있고, 제대혈(탯줄혈액), 세포·줄기세포, 난자 등은 체세포복제, 체세포핵이식, 단성생식 등의 연구에 없어서는 안 될 중요한 연구검체임
- 특히 줄기세포, 체세포복제 등의 연구는 루게릭병 등 난치 또는 불치병을 치료할 수 있는 유일한 탈출구로 여겨질 만큼 의료계의 기대가 크며, 따라서 세계 각국은 경쟁적으로 이 분야의 연구에 뛰어 들고 있음
- 그러나 이를 무제한으로 허용하면 장기, 제대혈(탯줄혈액), 세포·줄기세포, 난자, 정자 등이 무절제하게 거래되어 청소년, 여성, 가난한 사람 등의 인권을 침해할 수 있고, 차별적 행위의 결과를 낳을 수 있음
- 또한 유전자검사의 경우 칫솔, 타액, 머리카락 등의 검체 도용 피해도 적지 않으며 검사의 정확도도 많은 문제를 안고 있음

- 이와 같은 인권침해문제, 생명윤리문제, 여성 또는 약자의 건강권 문제, 종교적 문제 등으로 인해 생명윤리법 등은 인간과 인체유래물 등의 연구나 배아, 유전자 등의 취급을 엄격히 제한하고 있음

2) 유전자치료 연구범위의 확대

- 국내에서는 유전자치료의 범위가 「생명윤리 및 안전에 관한 법률」 제47조에 따라 “유전질환, 암, 후천성면역결핍증, 그 밖에 생명을 위협하거나 심각한 장애를 불러일으키는 질병의 치료를 위한 연구로서, 현재 이용 가능한 치료법이 없거나 유전자치료의 효과가 다른 치료법과 비교하여 현저히 우수할 것으로 예측되는 치료를 위한 연구”에 해당하는 경우에만 가능함

<< 생명윤리 및 안전에 관한 법률 >>

제 2 조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

16. “유전자치료”란 질병의 예방 또는 치료를 목적으로 인체 내에서 유전적 변이를 일으키거나, 유전물질 또는 유전물질이 도입된 세포를 인체로 전달하는 일련의 행위를 말한다.

제47조(유전자치료) ① 인체 내에서 유전적 변이를 일으키는 일련의 행위에 해당하는 유전자 치료에 관한 연구는 다음 각 호의 모두에 해당하는 경우에만 할 수 있다.

1. 유전질환, 암, 후천성면역결핍증, 그 밖에 생명을 위협하거나 심각한 장애를 불러일으키는 질병의 치료를 위한 연구
2. 현재 이용 가능한 치료법이 없거나 유전자치료의 효과가 다른 치료법과 비교하여 현저히 우수할 것으로 예측되는 치료를 위한 연구

② 유전물질 또는 유전물질이 도입된 세포를 인체로 전달하는 일련의 행위에 해당하는 유전자치료에 관한 연구는 제1항제1호 또는 제2호 중 어느 하나에 해당하는 경우에만 할 수 있다.

③ 유전자치료는 배아, 난자, 정자 및 태아에 대하여 시행하여서는 아니 된다.

○ 즉, 우리나라는 2015년 12월 생명윤리법 개정안에 대한 국회 심의 시 유전자연구를 인체 내에서 유전적 변이를 일으키는 행위와 단순히 유전물질을 인체로 전달하는 행위로 구분하여 연구 허용기준을 다르게 규정하기로 함

- 임상적 안전성이 확보되지 않은 유전적 변이를 일으키는 행위는 현재와 같이 ① 암, 유전질환 등 생명을 위협하는 질병치료 연구로서 ② 기존 치료법이 없거나 치료효과가 현저히 우수할 것으로 예측되는 치료 연구라는 두 가지 조건을 모두 충족하도록 하되, 단순히 유전물질을 인체로 전달만 하는 행위는 두 조건 중 하나만 충족해도 연구가 가능하도록 차등화함

⇒ OECD 국가 중 유전자치료의 연구범위를 법률로 정해 특정 질환으로 규제를 하고 있는 나라는 없음. 영국, 미국 등은 배아가 아닌 체세포 대상 유전자 치료의 연구범위만 제한하고 있으며, 임상시험 승인(FDA 등) 과정을 통해 안전성을 확보해야 함. 일본의 경우도 최근 유전자 치료 연구범위 제한 규정 폐지함('15.8)

⇒ 연구단계부터 불확실한 리스크에 근거하여 연구 범위를 일률적으로 제한하게 되면, 해당 분야에 대한 불확실성을 키워 의학 및 과학 발전을 저해하므로 글로벌 스탠다드에 맞게 수정할 필요가 있음

3) 비동결난자의 연구목적 사용 허용

○ 생명윤리법 제26조는 임신목적으로 생성되어 보존기간이 지나 폐기예정인 잔여 난자만을 연구에 사용할 수 있도록 제한하고 있음.

즉 체세포핵이식행위 또는 단성생식행위 연구시 동결란 또는 비정상 난자, 수정실패 난자 등만 이용토록 규정함(시행령 제14조)

- '05년 황우석 교수가 연구원 난자를 이용하고 난자 공여 시 금전적 이득을 제공한 사실이 사회적으로 문제를 야기한 바 있음

<< 생명윤리 및 안전에 관한 법률 >>

법 제26조(잔여배아 및 잔여난자의 제공) ① 배아생성의료기관은 연구에 필요한 잔여배아를 제30조제1항에 따라 배아연구계획서의 승인을 받은 배아연구기관에 제공하거나 잔여난자를 제31조제4항에 따라 체세포복제배아 등 연구계획서의 승인을 받은 체세포복제배아등의 연구기관에 제공하는 경우에는 무상으로 하여야 한다. 다만, 배아생성의료기관은 잔여배아 및 잔여난자의 보존 및 제공에 든 경비의 경우에는 보건복지부령으로 정하는 바에 따라 제공받는 연구기관에 대하여 경비지급을 요구할 수 있다.

시행령 제14조(체세포핵이식행위 또는 단성생식행위의 제한) ① 법 제31조제2항에 따라 체세포핵이식행위 또는 단성생식행위를 할 수 있는 연구는 다음 각 호의 요건을 모두 충족하여야 한다.

2. 다음 각 목의 어느 하나에 해당하는 난자를 이용하는 연구

- 가. 배아생성을 위하여 동결 보존된 난자 중에 임신이 성공되는 등의 사유로 폐기할 예정인 난자
- 나. 미성숙 난자 또는 비정상적인 난자로서 배아를 생성할 계획이 없어 폐기할 예정인 난자
- 다. 체외수정기술에 사용된 난자로서 수정이 되지 아니하거나 수정을 포기하여 폐기될 예정인 난자
- 라. 난임(難妊)치료를 목적으로 채취된 난자로서 적절한 수증자(受贈者)가 없어 폐기될 예정인 난자
- 마. 적출된 난소에서 채취한 난자

- 그러나 우리나라의 경우 경쟁국과 비교하여 비동결난자의 연구목적 활용에 대한 규제가 지나치게 엄격하여 줄기세포 연구에 큰 장애가 되고 있음

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

구분	한 국	독 일	미 국	영 국	일 본
관련 법규	<ul style="list-style-type: none"> ▪ 생명윤리법 	<ul style="list-style-type: none"> ▪ The German Embryo Protection Law 	<ul style="list-style-type: none"> ▪ 州 단위로 연구용 난자 기증과 관련한 가이드라인 	<ul style="list-style-type: none"> ▪ 인간 수정 및 발생에 관한 법 	<ul style="list-style-type: none"> ▪ 인간수정배아를 생성하는 보조생식술 연구에 관한 윤리지침 등
신선 난자 연구 목적 사용	<ul style="list-style-type: none"> ▪ 제한적 허용 -연구목적 난자 채취 금지 -체외수정 후 폐기예정인 난자 사용 원칙 1) 체외수정 후 잔여 동결 난자 2) 비정상난자 3) 수정포기 난자 4) 난임 치료 용 채취 후 수증자 없는 난자 5) 적출난소에서 채취된 난자 -연구계획 복지부 승인 	<ul style="list-style-type: none"> ▪ 금지 -연구목적난자 기증자체 금지 -연구 필요시, 줄기세포주 수입해 사용 * 중앙 윤리 위 수입 승인 	<ul style="list-style-type: none"> ▪ 州마다 상이 -캘리포니아주, 뉴욕주 등 제한적 허용 -메사츄세츠주 금지 *(예)캘리포니아 : 일정한 절차와 요건 하에 체외수정 후 잔여 난자 또는 연구용으로 기증된 신선난자를 사용 가능 -SCRO¹⁾ 승인 *(FDA Title 21 CFR screening test 에서 부적합한 것으로 판명된 기증 생식 세포는 포식라벨을 붙여 비임상적 사용 가능 	<ul style="list-style-type: none"> ▪ 제한적 허용 -연구목적으로 기증된 신선난자 사용 가능 -HFEA²⁾ 연구 계획 승인 	<ul style="list-style-type: none"> ▪ 제한적 허용 -연구목적 난자 채취 금지 -체외수정 후 폐기예정인 난자 사용 원칙 -단, 체외수정 목적으로 채취한 난자 중 다음은 비동결난자 사용 가능 1) 체외수정에 사용한 난자 중 수정되지 않은 것 2) 비정상 난자로 체외수정에 사용할 수 없는 것 3) 기증자가 연구에 제공할 뜻을 밝힌 것 4) 적출난소에서 채취된 난자 -연구계획 후생노동성 승인

구분	한 국	독 일	미 국	영 국	일 본
기증 자 보상	실비보상		실비보상 *ASRM윤리위 권고에 따르 면 상한 5,000 불/례) *체외수정 후 잔여난자를 기 증하면 시술비 감면 등을 하는 경우도 있음	실비보상 (750유로/회)	실비보상

- 난자는 동결-해동 과정에서 난자의 질이 떨어져 정상적인 신선난자와 비교하여 상대적으로 실험결과 도출이 어려움
 - 현재 미국과 한국에서만 체세포 복제 배아 줄기세포주 제작에 성공하였으며, 전반적 줄기세포치료기술은 세계 3위 수준임
 - 국내 차병원 연구팀은 국내에서 신선난자 이용 금지가 거듭된 연구실패 원인으로 보고 난자 기증이 가능한 미국에서 연구를 수행하여 세계에서 2번째로 인간체세포복제 배아줄기세포 생산에 성공('14.4)
 - ⇒ 난자 획득 과정에서의 윤리성이 확보된 경우 “비동결난자”의 연구 사용을 경쟁국 수준으로 허용하여야 함. 다만 비동결 난자의 이용을 허용할 경우, 난자 획득과정에서 금전적 거래가 이루어지거나 의도적으로 난자를 과다 생산해 난소과자극증후군, 경계성 난소종양, 조기폐경, 구토·현기증·무력감 등 여성의 건강이 문제될 수 있으므로 이에 대한 안전장치가 필요함

1) Stem cell Research Oversight Committee
2) Human Fertilisation Embryology Authority

⇒ 비동결 난자의 연구 목적 사용을 무조건 허용하는 것이 아니라, 임신을 위한 수정 후 남은 난자(비동결 잔여난자)로 한정해서 여성의 동의를 받아 사용을 허용함. 현재 기술적으로 배란·수정 후 잔여난자 발생 시 연구목적 사용에 대한 사후동의를 요청할 수 있고, 24시간 내 처리 가능함

4) 잔여배아의 연구 대상 확대

- 현재 국내에서는 잔여배아에 대한 연구가 생명윤리법 제29조제1항 및 시행령 제12조제1항에서 정하는 목적으로만 한정적으로 허용이 되고 있음
- 즉 난임치료법 및 피임기술의 개발 연구, 근이영양증, 그 밖에 대통령령으로 정하는 희귀·난치병의 치료 연구, 국가위원회의 심의를 거쳐 대통령령으로 정하는 연구로 한정됨

<< 생명윤리 및 안전에 관한 법률 >>

법 제29조(잔여배아 연구) ① 제25조에 따른 배아의 보존기간이 지난 잔여배아는 발생학적으로 원시선(原始線)이 나타나기 전까지만 체외에서 다음 각 호의 연구 목적으로 이용할 수 있다.

1. 난임치료법 및 피임기술의 개발을 위한 연구
2. 근이영양증(筋異營養症), 그 밖에 대통령령으로 정하는 희귀·난치병의 치료를 위한 연구
3. 그 밖에 국가위원회의 심의를 거쳐 대통령령으로 정하는 연구

시행령 제12조(잔여배아의 연구 대상인 희귀·난치병 등) ① 법 제29조제1항제2호에서 “대통령령으로 정하는 희귀·난치병”이란 다음 각 호에 해당하는 질병을 말한다.

1. 희귀병
 - 가. 다발경화증, 헌팅턴병(Huntington’s disease), 유전성 운동실조, 근위축성 측삭경화증, 뇌성마비, 척수손상

- 나. 선천성면역결핍증, 무형성빈혈, 백혈병
- 다. 골연골 형성이상

2. 난치병

- 가. 심근경색증
- 나. 간경화
- 다. 파킨슨병, 뇌졸중, 알츠하이머병, 시신경 손상
- 라. 당뇨병

- 생명윤리법이 잔여배아 연구 대상 질병의 범위를 제한하는 이유는 배아의 윤리적 획득과 남용 방지를 위한 것으로
 - 배아는 착상시 태아로 성장이 가능한 바, 대상질환의 특성, 치료 방법 연구 활용의 불가피성·시급성 등을 고려하여 연구대상 질병의 범위를 결정할 필요가 있고
 - 의료계에서 요구하고 있는 AIDS는 후천적 감염 바이러스성 질환으로 다양한 치료제가 이미 시판 중이거나 임상연구 중이고, 적절한 치료를 통해 관리가능하며, 보균상태로 30년 이상 생존이 가능해 배아를 활용하여 연구할 필요성이 타 질환보다 높지 않다고 보고 있음
- ⇒ 배아의 연구 목적 이용은 윤리적 문제가 있는 것은 사실이나, 연구대상 질병의 범위를 제한하여 연구자의 창의적인 연구까지 제약을 받는 것은 바람직스럽지 못함. 현시점의 의료기술에 비추어 효과를 기대하기 어렵더라도, 연구자가 스스로 판단하여 진행할 연구 자체를 금지할 필요는 없음.
- ⇒ 연구의 범위에 대한 논의는 국가생명윤리심의위원회의가 결정하거나 의료기간 내에 설치된 IRB(Institutional Review Board)에 맡기는 것이 바람직하고 이를 법률로 규제할 사항은 아님
- * IRB(기관생명윤리위원회): 인간을 대상으로 하는 시험에서 피시험자의 권리와 안전을 보호하기 위해 의료기관 내에 독립적으로 설치한 상설위원회. 연구 계획에 관한 윤리적, 과학적 타당성 등을 심의

Ⅲ. 수사분야

- 최근 10년도 넘은 미제사건이 유전자 검사를 통해 해결되는 등 범 죄수사 분야에서 생체정보의 이용 매우 활발함
- ‘디엔에이신원확인정보의 이용 및 보호에 관한 법률’ 제5조는 일단 한번이라도 죄를 지으면 모두 재범 가능성이 있는 것으로 보고 수 형인등으로부터의 디엔에이감식시료 채취를 폭넓게 인정하고 있음. 그러나 디엔에이 데이터베이스의 관리·운영에 대한 적절한 관리·감독 체계가 마련되어 있지 아니하여 사실상 경찰과 검찰의 자율에 맡겨져 있음
- 한편 ‘형사사법절차 전자화 촉진법’에 따른 ‘형사사법정보시스템’ 도 형사사법정보의 전자화에만 관심이 있고, 누구에 관하여, 어떤 정보가, 어떻게, 언제까지, 어떤 방식으로, 어떤 목적을 위해 이용 되고 있는지 공개되어 있지 아니하고 관리·감독 체계가 전무함
=> 양 법률 국민의 기본권을 심각하게 침해할 우려가 있으므로 그 운영 및 관리의 투명성을 확보하고, 독립적이고 객관적인 관리·감독 시스템이 필요함

——— << 생명윤리 및 안전에 관한 법률 >> ———

제14조(디엔에이신원확인정보데이터베이스관리위원회) ① 데이터베이스의 관리·운영에 관한 다음 각 호의 사항을 심의하기 위하여 국무총리 소속으로 디엔에이신원확인정보데이터베이스관리위원회(이하 "위원회"라 한다)를 둔다.

1. 디엔에이감식시료의 수집, 운반, 보관 및 폐기에 관한 사항
2. 디엔에이감식의 방법, 절차 및 감식기술의 표준화에 관한 사항
3. 디엔에이신원확인정보의 표기, 데이터베이스 수록 및 삭제에 관한 사항

4. 그 밖에 대통령령으로 정하는 사항

② 위원회는 위원장 1명을 포함한 7명 이상 9명 이하의 위원으로 구성한다.

③ 위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 국무총리가 위촉하며, 위원장은 국무총리가 위원 중에서 지명한다.

1. 5급 이상 공무원(고위공무원단에 속하는 일반직공무원을 포함한다) 또는 이에 상당하는 공공기관의 직에 있거나 있었던 사람으로서 디엔에이와 관련한 업무에 종사한 경험이 있는 사람

2. 대학이나 공인된 연구기관에서 부교수급 이상 또는 이에 상당하는 직에 있거나 있었던 사람으로서 생명과학 또는 의학 분야에서 전문지식과 연구경험이 풍부한 사람

3. 그 밖에 윤리학계, 사회과학계, 법조계 또는 언론계 등 분야에서 학식과 경험이 풍부한 사람

④ 위원의 임기는 3년으로 한다.

⑤ 위원회는 제1항 각 호 사항의 심의에 필요하다고 인정하는 때에는 검찰총장 및 경찰청장에게 관련 자료의 제출을 요청할 수 있고, 디엔에이신원확인정보담당자 등을 위원회의 회의에 참석하게 하여 의견을 들을 수 있다.

⑥ 위원회는 제1항 각 호의 사항을 심의하여 검찰총장 또는 경찰청장에게 의견을 제시할 수 있다.

⑦ 제1항부터 제6항까지에서 규정한 사항 외에 대통령령으로 정한다.

※ 의료분야의 이슈는 발표자가 위원으로 활동하고 있는 국무조정실
신산업투자위원회의 자료를 일부 활용한 것임

생체정보의 분야별 활용현황 - 의료분야

배 현 아
(이화여자대학교 생명의료법연구소 교수)

생체정보의 활용 및 보호를 위한 법제 정비방안 연구 :생체정보의 분야별 활용현황-의료

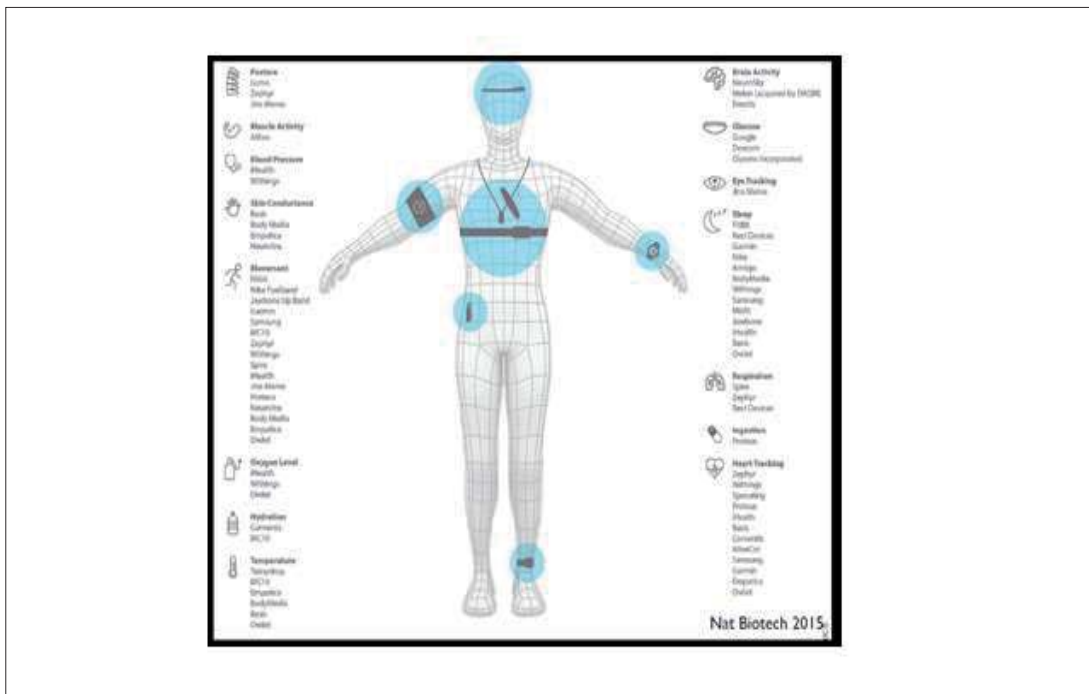
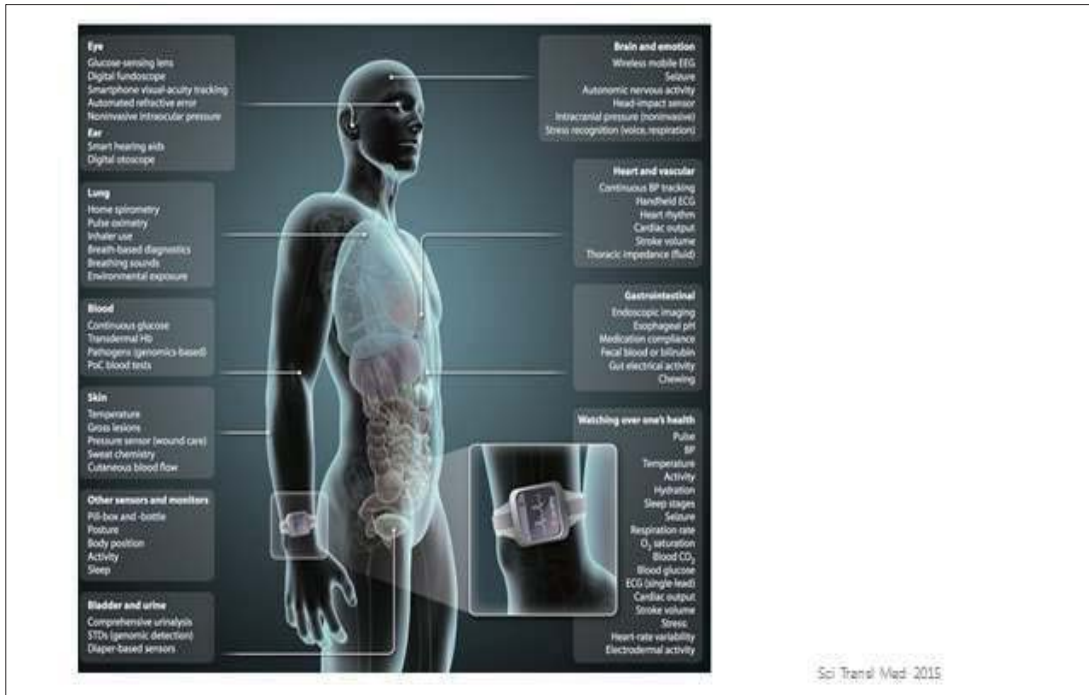
이화여자대학교 법학전문대학원
생명의료법연구소
배현아

2016-05-17

생체정보

- 지문, 홍채, 망막, 얼굴, 음성, 손모양, 손혈관, 서명 등 개인의 일정한 생체적 특성들
- 생체정보를 측정 후 이를 **데이터베이스화**하고 이를 통하여 그 개인을 인식(이른바 생체인식 기술)
 - 전자화된/빅데이터/위·변조 대량 유출 위험성
- 신체적 특징
 - 지문, 손모양, 얼굴, 홍채, DNA 등
- 행동적 특징
 - 성문, 서명, 걸음거리
- 보건의료법제 내에서 생체정보의 개념/수집 가능한 정보의 범위/수단/행위
- 생체정보-개인(식별)정보-진료(의료)정보-유전정보

생체정보의 활용 및 보호를 위한 법제 정비방안 연구



생체정보의 특징

- **개인식별정보/의료내용에 관한 정보**
 - 대법원 2013.12.12, 선고, 2011도9538, 판결
 - "전자의무기록에 저장된 '개인정보'에는 환자의 이름·주소·주민등록번호 등과 같은 '개인식별정보'뿐만 아니라 환자에 대한 진단·치료·처방 등과 같이 공개로 인하여 개인의 건강과 관련된 내밀한 사항 등이 알려지게 되고, 그 결과 인격적·정신적 내면생활에 지장을 초래하거나 자유로운 사생활을 영위할 수 없게 될 위험성이 있는 의료내용에 관한 정보도 포함된다."
- **사람과 불가분으로 결합**
 - 예. 유전정보
- **절대적으로 변경이 불가능**
 - 익명화

생체정보를 포함하는 진료정보

- **의료기관에서 생성, 이용되고 있는 의무기록(진료)정보**
- **환자의 과거병력, 증상, 가족력 등의 개인정보를 바탕으로**
- **의사의 전문적 의학지식이 더해져 생성되는 정보**
- **의학적, 교육적, 공중보건 및 보건정책면에서 활용되어야 할 사회의 공공재**

진료정보 관련 법제 (1)

제22조(진료기록부 등) ① 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)을 갖추어 두고 환자의 주된 증상, 진단 및 치료 내용 등 보건복지부령으로 정하는 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다.

② 의료인이나 의료기관 개설자는 진료기록부등[제23조제1항에 따른 전자의무기록(電子醫務記錄)을 포함한다. 이하 제40조제2항에서 같다]을 보건복지부령으로 정하는 바에 따라 보존하여야 한다.

③ 의료인은 진료기록부등을 거짓으로 작성하거나 고의로 사실과 다르게 추가·기재·수정하여서는 아니 된다.

제23조(전자의무기록)

전자의무기록

제23조(전자의무기록) ① 의료인이나 의료기관 개설자는 제22조의 규정에도 불구하고 진료기록부등을 「전자서명법」에 따른 전자서명이 기재된 전자문서(이하 "전자의무기록"이라 한다)로 작성·보관할 수 있다.

② 의료인이나 의료기관 개설자는 보건복지부령으로 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는 데에 필요한 시설과 장비를 갖추어야 한다.

③ 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.

- 제14조(진료기록부 등의 기재 사항) ④ 법 제22조제1항에 따라 진료기록부·조산기록부와 간호기록부(이하 "진료기록부들"이라 한다)에 기록해야 할 의료행위에 관한 사항과 의견은 다음 각 호와 같다.
1. 진료기록부
 - 가. 진료를 받은 사람의 주소·성명·연락처·주민등록번호 등 인적사항
 - 나. 주된 증상 이 경우 의사가 필요하다고 인정하면 주된 증상과 관련된 영적(靑瘧)가위력(康復力)중 추가를 기록할 수 있다.
 - 다. 진단결과 또는 진단일
 - 라. 진료결과(의뢰항자는 개인정보처리서 증상 상태, 치료내용이 변동되어 의사가 그 변동중 기록할 필요가 있다고 인정하는 환자만 해당한다)
 - 마. 치료 내용(주사 투약 처치 등)
 - 바. 진료 일시(日時)
 2. 조산기록부
 - 가. 조산중 받은 자의 주소·성명·연락처·주민등록번호 등 인적사항
 - 나. 산·사산(産) 胎(胎) 産(産) 後(後) 處(處) 理(理) 處(處) 方(方)
 - 다. 임신 중의 경과와 그에 대한 소견
 - 라. 임신 중 의사에 의한 건강진단의 유무(유후) 및 성별에 관한 검사등 포함한다.
 - 마. 분만 장소 및 분만 방법(産科) 處(處) 方(方)
 - 바. 분만의 결과 및 그 처치사. 산아(産兒) 수와 그 성별 및 성사의 구별사. 산아와 태아부속물에 대한 소견
 - 자. 석계
 - 차. 산후의 의사의 건강진단 유무
 3. 간호기록부
 - 가. 간호를 받은 사람의 성명
 - 나. 체온·혈압·호흡·말합에 관한 사항
 - 다. 투약에 관한 사항
 - 라. 섭취 및 배설물에 관한 사항
 - 마. 처치와 간호에 관한 사항
 - 바. 간호 일시(日時)

진료정보 관련 법제 (2)

- 제17조(진단서 등) ① 의료업에 종사하고 직접 진찰하거나 검안(檢案)한 의사[이하 이 항에서는 검안서에 한하여 검시(檢屍)업무를 담당하는 국가기관에 종사하는 의사를 포함한다], 치과의사, 한의사가 아니면 진단서·검안서·증명서 또는 처방전(의사나 치과의사가 「전자서명법」에 따른 전자서명이 기재된 전자문서 형태로 작성한 처방전(이하 "전자처방전"이라 한다)을 포함한다. 이하 같다)을 작성하여 환자(환자가 사망한 경우에는 배우자, 직계존비속 또는 배우자의 직계존속을 말한다) 또는 「형사소송법」 제222조제1항에 따라 검시(檢屍)를 하는 지방검찰청검사(검안서에 한한다)에게 교부하거나 발송(전자처방전에 한한다)하지 못한다. 다만, 진료 중이던 환자가 최종 진료 시부터 48시간 이내에 사망한 경우에는 다시 진료하지 아니하더라도 진단서나 증명서를 내줄 수 있으며, 환자 또는 사망자를 직접 진찰하거나 검안한 의사·치과의사 또는 한의사가 부득이한 사유로 진단서·검안서 또는 증명서를 내줄 수 없으면 같은 의료기관에 종사하는 다른 의사·치과의사 또는 한의사가 환자의 진료기록부 등에 따라 내줄 수 있다.
- 제19조(비밀 누설 금지) 의료인은 이 법이나 다른 법령에 특별히 규정된 경우 외에는 의료·조산 또는 간호를 하면서 알게 된 다른 사람의 비밀을 누설하거나 발표하지 못한다.

진료정보 관련 법제 (3)

제21조(기록 열람 등) ① 의료인이나 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다.

② 제1항에도 불구하고 의료인이나 의료기관 종사자는 다음 각 호의 어느 하나에 해당하면 그 기록을 열람하게 하거나 그 사본을 교부하는 등 그 내용을 확인할 수 있게 하여야 한다. 다만, 의사치과의사 또는 한의사가 환자의 진료를 위하여 불가피하다고 인정한 경우에는 그러하지 아니하다...[중략]

③ 의료인은 다른 의료인으로부터 제22조 또는 제23조에 따른 진료기록의 내용 확인이나 환자의 진료경과에 대한 소견 등을 승부할 것을 요청받은 경우에는 해당 환자나 환자 보호자의 동의를 받아 승부하여야 한다. 다만, 해당 환자의 의식이 없거나 응급환자인 경우 또는 환자의 보호자가 없어 동의를 받을 수 없는 경우에는 환자나 환자 보호자의 동의 없이 승부할 수 있다.

④ 진료기록을 보관하고 있는 의료기관이나 진료기록이 보관된 보건소에 근무하는 의사치과의사 또는 한의사는 자신이 직접 진료하지 아니한 환자의 과거 진료 내용의 확인 요청을 받은 경우에는 진료기록을 근거로 하여 사실을 확인하여 줄 수 있다.

⑤ 의료인은 **응급환자**를 다른 의료기관에 이송하는 경우에는 지체 없이 내원 당시 작성된 진료기록의 사본 등을 이송하여야 한다.

생체정보/진료정보와 관련된 권리·의무(1)

- 의료소비자/의료제공자
- 정보자기결정권/자기정보관리 통제권
 - 자신에 관한 정보가 언제 어떻게 그리고 어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 자율적으로 결정할 수 있는 권리
 - 자기정보 열람청구권/자기정보 정정청구권/자기정보 사용중지·삭제청구권
- 진료정보의 소유권
 - 진료기록을 작성한 의료기관(의료인)/정보의 대상이 되는 환자
 - 진료기록에 관한 의무와 권리

의료기관(의료인)의 진료기록 소유권 인정 근거

- 진료기록은 의료인간의 의사소통 수단으로 환자 진료 **지속성** 확보를 위한 주요 수단
- 진료기록에 기록된 자료는 의료종사자들의 진료의 질 보장, 평가 및 향상을 위한 연구에 필요한 정보를 제공
- 의료기관의 진료수행에 대한 증거가 되어 보험청구를 위한 기본자료
- 법적인 자료로서 의료의 거래에 있어서 의료인과 환자를 동시에 보호하는 역할

생체정보/진료정보와 관련된 권리·의무(2) : 개인정보 보호 관련 법제

- 헌법 제17조 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.
- 개인정보보호법
 - 개인정보의 수집, 이용, (제3자) 제공 등
 - 개인정보의 목적 외 이용 제한
 - 민감정보의 처리 제한
 - 건강에 관한 정보
 - 고유식별정보의 처리 제한
 - 주민등록번호 처리의 제한
 - (별도의) 동의/법률에 근거/업무 수행 등
- 법령 자체에 법령에서 사용하는 용어의 정의나 포섭의 구체적인 범위가 명확히 규정되어 있지 아니한 경우,

[대법원 1997.8.29, 선고, 97도1234, 판결]

- 의사가 환자를 진료하는 경우에는 의료법 제21조 제1항에 의하여 그 의료행위에 관한 사항과 소견을 상세히 기록하고 서명한 진료기록부를 작성하여야 하고, 진료기록부를 작성하지 않은 자는 같은 법 제69조에 의하여 처벌하도록 되어 있는바, 이와 같이 **의사에게 진료기록부를 작성하도록 한 취지는 ①진료를 담당하는 의사 자신으로 하여금 환자의 상태와 치료의 경과에 관한 정보를 빠뜨리지 않고 정확하게 기록하여 이를 그 이후의 계속되는 환자치료에 이용하도록 함과 아울러 다른 관련 의료종사자에게도 그 정보를 제공하여 환자로 하여금 적절한 의료를 제공받을 수 있도록 하고, ②의료행위가 종료된 이후에는 그 의료행위의 적정성을 판단하는 자료로 사용할 수 있도록 하고자 함에 있다.**

정보 교류를 전제로 한 정보의 수집

- Health **Information Exchange**
 - **The electronic** movement of health-related information among organizations according to nationally recognized standards
 - Safer, timelier, efficient, effective, equitable, patient-centered care
- Benefit
 - Improving health care
 - Improving health and decreasing costs by putting vital health information in the hands of clinicians
 - Reduced hospital admissions and duplicate testing
- Secondary Use
 - Quality measurement and improvement, disaster management, public health and research
- Health information exchange network: real-time community-wide clinical data set
- Query based exchange/directed exchange between providers/consumer mediated exchange with online access to their health information

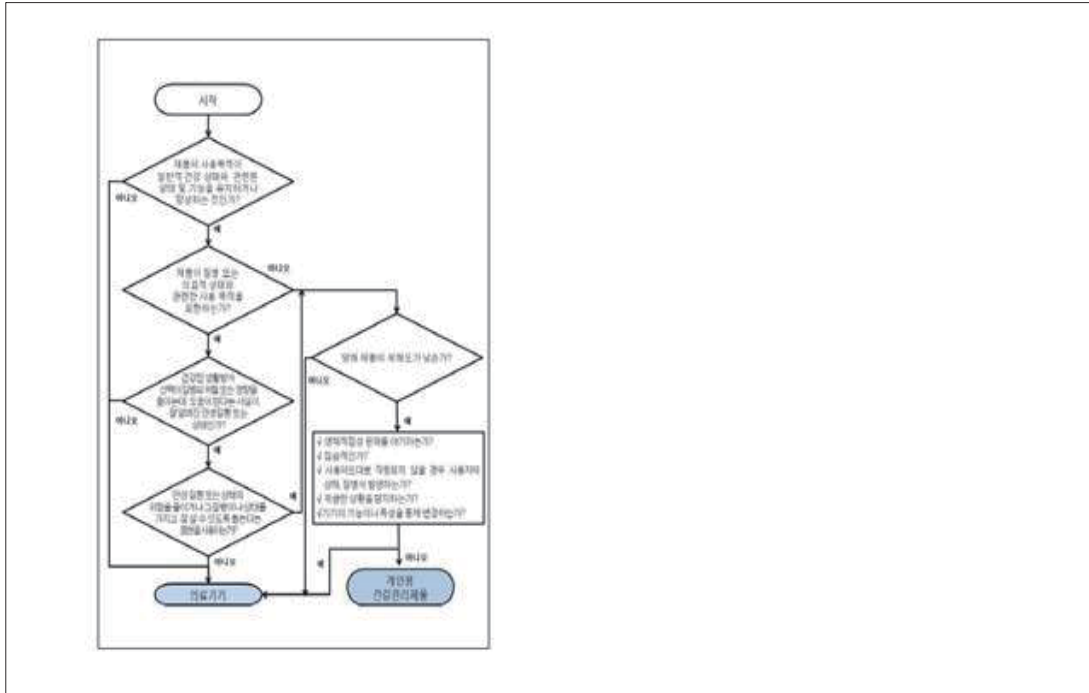
Jason SS, et al. Health Information Exchange in Emergency Medicine. Ann of Emerg Med. 2015

정보의 수집과 공유(exchange)를 통한 활용(예)

- 중증응급환자 등록 관리 프로그램
- 호흡감염 중증환자 추적 관리 프로그램
 - 감염병의 예방 및 관리에 관한 법률
 - 감염병에 관한 정보의 수집분석 및 제공
 - 감염병에 관한 조사연구
 - 감염병 관리정보 교류 등을 위한 국제협력
 - 국민의 알권리와 정보공개 의무
- 이송환자 의무기록 정보연계 프로그램
- 개인의무기록 정보제공 프로그램
- (응급의료)정보통신망

생체정보의 활용: 의료기기와 의료용 앱

- 의료기기의 정의 및 판단기준
 - 기구, 기계, 장치, 재료, 사용목적, 위험도
 - (의료용)소프트웨어
 - (의료용) 모바일 앱: 의료기기를 원격으로 제어하는 앱, 의료기기에서 측정된 데이터 등을 전송 받아 표시, 저장, 분석하는 앱, 모바일 플랫폼에 전극, 센서 등을 부착 또는 추가하여 모바일 플랫폼을 의료기기로 사용하는 앱, 모바일 플랫폼에 내장된 센서를 이용하여 모바일 플랫폼을 의료기기로 사용하는 앱
- 의료기기와 개인용 건강관리[웰니스]제품 판단기준[지침]2015.07.10
 - 운동레저 및 일상적 건강관리 목적의 개인용 건강관리제품의 구분
 - 일상적 건강관리용/만성질환자 자가관리용
 - General Wellness: Policy for Low Risk Devices
- 모바일 의료용 앱 안전관리 지침(2013.12)
- Wearable device



신의료기술의 평가

구 분	평가제도(허가제도)		급여결정제도
	식약처 (A)	신의료기술 평가위원회 (B) (NECA)	의료행위 전문평가위원회 (C) (HIRA)
관련법령	약사법 의료기기법	의료법	건강보험법
내용	안전성·유효성 평가		경제성·급여적정성평가
대상	의약품, 의료기기	신의료기술	안전성, 유효성이 확인된 신의료기술
결과	허가 (시장진입허용)	보건복지부장관 고시 (건강보험 등재를 위한 필수요건)	보건복지부장관 고시 (건강보험 등재)
의미	국민건강권 보호 및 신의료기술 발전 촉진을 위한 국가적 검증체계		안전성·유효성이 검증된 신기술의 건강보험 적용

생체신호를 이용한 응급상황 예측 의료정보시스템

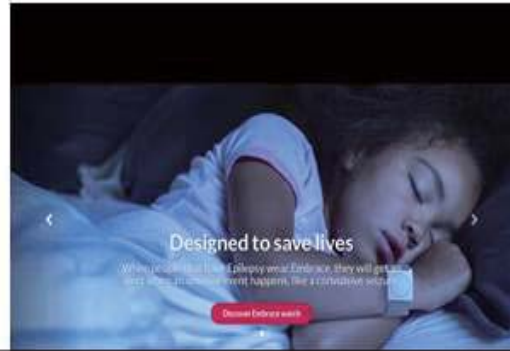
Ematrica E4 Specifications

- Battery life:** Sleeping Mode: 20+hrs, Memory mode: 6h+ hrs
- Data Management:** Flash memory, Bluetooth LE (Smart)
- Form Factor:** Sleek and comfortable, 1.5" x 0.5" x 0.2" (approximate)
- Event Mark Button:** (Physical button on the band)
- Certification:** CE certification, FCC certification
- Sensors:** Photoplethysmography (PPG), 3-axis Accelerometer, Temperature & Heart Rate, Electrodermal Activity (EDA)

Measure both branches of the autonomic nervous system.

Electrodermal Activity | **Continuous Heart Rate**

Smart Band detecting seizure



Your Smartphone Will See You Now

CellScope's iPhone-enabled otoscope

SpiroSmart: spirometer using iPhone

GluCase™ contains everything found in a traditional glucose meter kit.

앱+Wearable device



개인건강기록(Personal Health Record)

- **개인**이 건강에 대한 의사결정을 하기 위해 필요한 **언제 어디에 서나** 이용 가능한 **평생** 건강정보의 공급원
 - 개인의 평생 건강기록
 - 개인의 통합적이고 포괄적인 건강기록
 - 개인이나 개인이 지정한 대리인이 건강정보의 통제권을 가짐
 - 언제 어디서나 건강정보에 접근할 수 있고 이를 검색하거나 전송할 수
 - 개인이 직접 건강정보를 입력하거나 다양한 보건의료서비스 제공자로부터 제공 받음
 - 개인이 자신의 건강을 최적으로 관리하도록 도와주는 건강관리도구

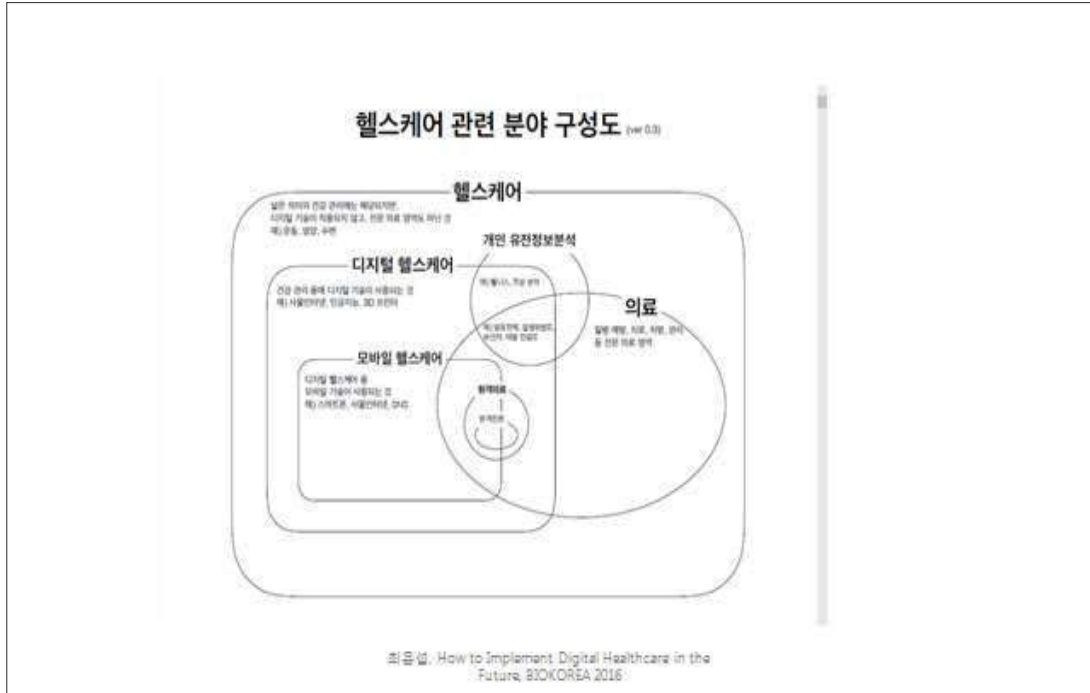
Mayo clinic application

- Created in collaboration with Apple and Mayo Clinic
- 2012.5- 현재



<http://www.mayoclinic.org/apps/mayo-clinic>





의료법 제34조 원격의료

- ① 의료인(의료업에 종사하는 의사·치과의사·한의사만 해당한다)은 제33조제1항에도 불구하고 컴퓨터·화상통신 등 정보통신기술을 활용하여 먼 곳에 있는 의료인에게 의료지식이나 기술을 지원하는 원격의료(이하 "원격의료"라 한다)를 할 수 있다.
- ② 원격医료를 행하거나 받으려는 자는 보건복지부령으로 정하는 시설과 장비를 갖추어야 한다.
- ③ 원격医료를 하는 자(이하 "원격지의사"라 한다)는 환자를 직접 대면하여 진료하는 경우와 같은 책임을 진다.
- ④ 원격지의사의 원격의료에 따라 의료행위를 한 의료인이 의사·치과의사 또는 한의사(이하 "현지의사"라 한다)인 경우에는 그 의료행위에 대하여 원격지의사의 과실을 인정할 만한 명백한 근거가 없으면 환자에 대한 책임은 제3항에도 불구하고 현지의사에게 있는 것으로 본다.

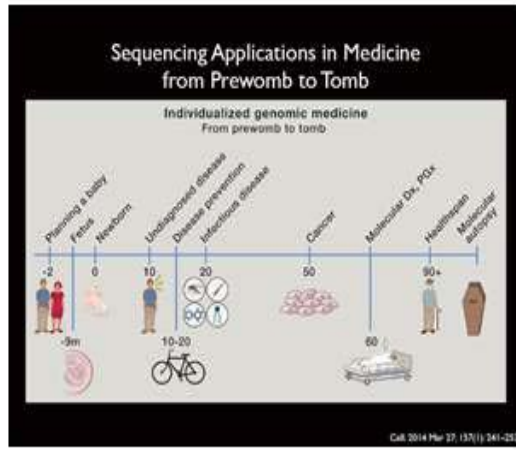
[대법원 2013.12.12, 선고, 2011도9538, 판결]

- 법령 자체에 법령에서 사용하는 용어의 정의나 포섭의 구체적인 범위가 명확히 규정되어 있지 아니한 경우, 그 용어가 사용된 법령 조항의 해석은 그 법령의 전반적인 체계와 취지·목적, 당해 조항의 규정 형식과 내용 및 관련 법령을 종합적으로 고려하여 해석하여야 한다. 이러한 법리를 의료법의 개정 연혁, 내용 및 취지, 의료법 제22조 제1항, 제3항, 제23조 제1항, 제3항, 구 의료법(2011. 4. 7. 법률 제10565호로 개정되기 전의 것) 제66조 제1항 제3호, 의료법 시행규칙 제14조 제1항 제1호, 제3호의 규정, 의무기록에 기재된 정보와 사생활의 비밀 및 자유와의 관계 등에 비추어 보면, 의료법 제23조 제3항의 적용 대상이 되는 전자의무기록에 저장된 '개인정보'에는 환자의 이름·주소·주민등록번호 등과 같은 '개인식별정보'뿐만 아니라 환자에 대한 진단·치료·처방 등과 같이 공개로 인하여 개인의 건강과 관련된 내밀한 사항 등이 알려지게 되고, 그 결과 인격적·정신적 내면생활에 지장을 초래하거나 자유로운 사생활을 영위할 수 없게 될 위험성이 있는 의료내용에 관한 정보도 포함된다고 새기는 것이 타당하다.
- 환자를 진료하 당해 의료인은 의무기록 작성권자로서 보다 정확하고 상세한 기재를 위하여 사후에 자신이 작성한 의무기록을 가필·정정할 권한이 있다고 보이는 점, 2011. 4. 7. 법률 제10565호로 의료법을 개정하면서 허위 작성 금지규정(제22조 제3항)을 신설함에 따라 의료인이 고의로 사실과 다르게 자신이 작성한 진료기록부 등을 추가·기재·수정하는 행위가 금지되었는데 이때의 진료기록부 등은 의무기록을 가리키는 것으로 불이 타당한 점, 문서변조죄에 있어서 통상적인 변조의 개념 등을 종합하여 보면, 전자의무기록을 작성한 당해 의료인이 그 전자의무기록에 기재된 의료내용 중 일부를 추가·수정하였다 하더라도 그 의료인은 의료법 제23조 제3항에서 정한 변조행위의 주체가 될 수 없다고 보아야 한다.

[대법원 2013.12.12, 선고, 2011도9538, 판결]

- 전자의무기록은 의료정보화를 촉진하기 위하여 2002. 3. 30. 법률 제 6686호로 개정된 의료법에서 처음 규정되었고, 이로써 종래 문서 형태로 한정되던 진료기록부 등을 전자의무기록으로 대체할 수 있게
- 진료기록부 등과 전자의무기록(이하 통칭하여 '의무기록'이라 한다)에는 앞서 본 바와 같이 환자에 관한 다양한 정보가 기재되는데, 전자의무기록의 경우 전자문서의 속성상 진료기록부 등에 비하여 이들 정보가 손쉽게 위·변조되거나 대량으로 유출될 수 있는 위험성이 상존하고 있다. 이에 따라 위 의료법 개정 당시 전자의무기록에 관한 규정을 신설하면서 작성권자로 하여금 전자서명법에 따른 전자서명을 하도록 하는 한편 전자의무기록에 저장된 개인정보를 탐지, 누출, 변조 또는 훼손하는 행위를 금지하는 이 사건 규정을 신설하였다.

유전정보



생명윤리 및 안전에 관한 법률

- 제2조(정의) 14. "유전정보"란 인체유래물을 분석하여 얻은 개인의 유전적 특징에 관한 정보를 말한다.
- 제46조 유전정보에 의한 차별 금지
- 제47조 유전자치료
- 제48조 유전자치료기관
- 제49조 유전자검사기관
- 제50조 유전자검사의 제한
- 제51조 유전자검사의 동의

제50조 유전자검사의 제한 등

- ① 유전자검사기관은 과학적 증거가 불확실하여 검사대상자를 오도(誤導)할 우려가 있는 신체 외관이나 성격에 관한 유전자검사 또는 그 밖에 국가위원회의 심의를 거쳐 대통령령으로 정하는 유전자검사를 하여서는 아니 된다.
- ② 유전자검사기관은 근이영양증이나 그 밖에 대통령령으로 정하는 유전질환을 진단하기 위한 목적으로만 배아 또는 태아를 대상으로 유전자검사를 할 수 있다.
- ③ 의료기관이 아닌 유전자검사기관에서는 다음 각 호를 제외한 경우에는 질병의 예방, 진단 및 치료와 관련한 유전자검사를 할 수 없다. <개정 2015.12.29.>
 1. 의료기관의 의뢰를 받은 경우
 2. 질병의 예방과 관련된 유전자검사로 보건복지부장관이 필요하다고 인정하는 경우
- ④ 유전자검사기관은 유전자검사에 관하여 거짓표시 또는 과대광고를 하여서는 아니 된다. 이 경우 거짓표시 또는 과대광고의 판정 기준 및 절차, 그 밖에 필요한 사항은 보건복지부령으로 정한다.

The image shows a screenshot of the WADIZ website. On the left, there is a 23andMe logo and a line graph titled "Customer growth of 23andMe". The graph shows a steady increase in customer numbers from 2010 to 2015, with a significant spike in 2015. The y-axis represents the number of customers, ranging from 0 to 1,000,000. The x-axis represents the year. The data points are approximately: 2010: 100,000; 2011: 150,000; 2012: 200,000; 2013: 300,000; 2014: 400,000; 2015: 1,000,000.

The main content of the screenshot is a 23andMe advertisement. It features a central image of a person's face with various genetic traits highlighted. The text in the advertisement includes "나만을 위한 다이어트 방법, 유전자 맞춤 다이어트 솔루션 제공하는 곳" and "당신의 몸속으로 유전자 정보를 읽어, 맞춤 영양 정보를 제공한다".

On the right side of the screenshot, there is a sidebar with a search bar and a list of search results. The search results include various items such as "유전자 검사", "유전자 검사 방법", "유전자 검사 비용", "유전자 검사 결과", "유전자 검사 결과 해석", "유전자 검사 결과 공유", "유전자 검사 결과 저장", "유전자 검사 결과 삭제", "유전자 검사 결과 복구", "유전자 검사 결과 인쇄", "유전자 검사 결과 다운로드", "유전자 검사 결과 업로드", "유전자 검사 결과 공유 링크", "유전자 검사 결과 공유 링크 복사", "유전자 검사 결과 공유 링크 삭제", "유전자 검사 결과 공유 링크 복구", "유전자 검사 결과 공유 링크 인쇄", "유전자 검사 결과 공유 링크 다운로드", "유전자 검사 결과 공유 링크 업로드".

결론: 생체정보의 활용 및 보호를 위한 법제 정비(1)

- 생체정보의 특성과 활용가능성을 고려한 정의, 범주화
 - 개인 건강에 관한 민감한 정보
 - 환자 개인의 생명신체보호에 직접적인 영향을 줄 수
 - 강력한 보호/정보주체의 참여 보장
 - 국가보건정책 수립에 중요한 자원으로 이용될 수 있는 (준)공공재 차원의 특성
 - 이득의 수혜자 범위
 - 정보보호를 위하여 투입되어야 하는 비용부담의 책임과 수준
 - 정보주체(환자 본인)의 권리 행사의 적정범위에 대한 **사회적 합의**가 이루어져야 함
- 시간적인 요인
 - 원격의료(?)

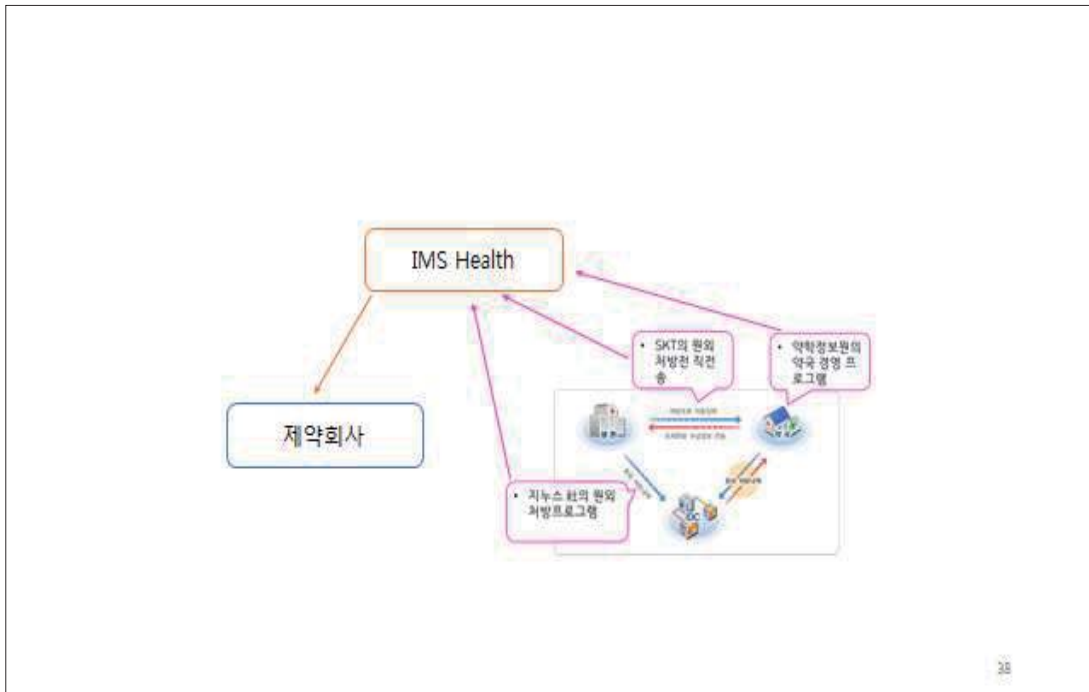
결론: 생체정보의 활용 및 보호를 위한 법제 정비(2)

- 다른 개인 소비분야 등의 개인정보와 달리 건강정보의 수집에 대한 동의, 열람 및 정정·삭제요청 등에 대하여 개인건강정보로서의 생체정보의 특성에 맞는 별도의 **정보주체의 참여기준**이 마련되어야
- 개인건강정보로서의 생체정보의 적절한 보호 및 관리를 위한 법적, 제도적 장치 필요
 - 생체정보 취급자 및 그 자격을 제한
 - 보호관리를 생체정보 관련기관 내부절차 강화
 - 기술적 대책
 - 관리적 보호조치(예. 개인정보보호위원회, 보안심사위원회)/물리적 보호조치(출입통제시스템, 보안담당자, PC 관리번호, 보안스티커, 비밀번호, IP 통제 등)/기술적 보호장치(업무망/인터넷망 네트워크 물리적 분리 등)
 - 개인정보보호 실태점검 및 인증 절차

결론: 생체정보의 활용 및 보호를 위한 법제 정비(3)

- 법령자체에 그 법령에서 사용하는 용어의 정의나 포섭의 구체적인 범위가 명확히 규정되어 있지 아니한 경우, 그 용어가 사용된 법령조항의 해석은 그 법령의 전반적인 체계와 취지목적, 당해 조항의 규정 형식 및 내용 및 관련 법령을 종합적으로 고려하여 해석하여야
 - 전자의무기록/개인의무기록(Personal Health Record)

- 의료관계법 개정 또는 입법을 통한 개인건강정보보호 체계 구축
 - 의료분야 정보화와 다양한 이해당사자 고려
 - 환자보호자, 의료기관종사자, 건강보험공단, 심평원, 약국, 타 의료기관, 정책당국 등
 - 의료기관들이 인터넷을 통해 환자에게 개인건강정보 제공
 - 1,2,3차 의료기관 간 의료협력 네트워크 상에서 개인건강정보의 공유가 증가
 - 다른 어떤 개인정보 관련 분야보다 복잡
 - 정보보호 관련 리스크에 대한 적절한 관리 필요



생체정보의 분야별 활용현황 - 범죄수사분야

정 소 영
(충남대 법학과 강사)

I . 생체정보(Bio Information)

□ 생체정보(Bio Information)의 분류¹⁾

- 개인 식별이나 인증을 위한 생체인식정보/바이오인식정보(biometric)
- 맥박, 심박동, 호흡, 심전도 등의 생체신호(bio-signal,/vital signal)
- 신장, 몸무게, 얼굴형태 등 신체외관정보

□ 생체정보(Bio Information)의 형사법적 활용 예

- 생체인식정보: 범죄자 식별, 범죄자 특정(지문/족형, 성문검사) 등에 사용
- 생체신호: 범죄 증거의 수집(거짓말탐지기), 범죄 징후의 발견(지능형 전자발찌, 뇌파측정)
- 신체외관정보: 체포/구속된 피의자에 대한 신장/체중 측정과 사진 촬영

□ 공공기관의 생체인식정보의 활용 예

- 법무부 출입국 관리 분야: 9.11 테러 이후 미국에서 생체여권 도입. 우리나라도 안면정보/지문정보를 등록한 사람에 한하여 자동출입국 제도 시행 중

1) 이원상, “빅데이터 환경에서 생체정보의 형사정책적 활용에 대한 고찰”, 비교형사법연구 17권 1호, 2015, 111면

- 경찰청 실종 아동 사전 등록: 『실종아동등의 보호 및 지원에 관한 법률』에 근거하여 2012년부터 시행. 보호자가 원하는 경우 지문, 사진, 보호자정보를 사전에 등록. 아동, 지적장애인, 치매환자의 실종 시 신속한 대응. 2015년 8월 기준 241만명 등록. 2015년 상반기 발생한 11세 미만의 실종 아동 2041명을 전원 찾았다고 함²⁾

II. 범죄·수사 분야의 생체신호 활용

□ 심리생리검사 (Polygraph Examination) - 일명 거짓말탐지기

- 거짓말을 할 때 나타날 수 있는 생리적 변화 가운데 호흡과 심장 박동 수, 혈압의 변화 등을 측정해 거짓말 여부를 가리는 장치
- 과학수사(Forensic Science³⁾)의 한 분야로, 형사소송법에서는 피검사자의 동의를 얻어 임의수사의 방식으로 허용
- 거짓말탐지기의 검사 결과는 아직 공소사실에 대한 직접증거로는 인정받지 못하고 있음.⁴⁾ 진술의 진위를 판단하는 근거로 사용

2) 파이낸셜뉴스 2015.8.1. 보도 “실종자 찾기, 우리 모두의 몫”

(<http://www.fnnews.com/news/201508071657143432>)

3) 과학수사 또는 법과학으로 번역되며, 미국의 형사대배심 제도와 유사하게 고대 로마에서 forum(포룸, 광장)에 시민들이 모여 범죄 증거 조사를 통해 형사기소를 하였던 것에서 유래하였다.

(<https://ko.wikipedia.org/wiki/%EB%B2%95%EA%B3%BC%ED%95%99>)

4) 대법원 2005. 5. 26. 선고 2005도130 판결

【판결요지】

[1] 거짓말탐지기의 검사 결과에 대하여 사실적 관련성을 가진 증거로서 증거능력을 인정할 수 있으려면, 첫째로 거짓말을 하면 반드시 일정한 심리상태의 변동이 일어나고, 둘째로 그 심리상태의 변동은 반드시 일정한 생리적 반응을 일으키며, 셋째로 그 생리적 반응에 의하여 피검사자의 말이 거짓인지 아닌지가 정확히 판정될 수 있다는 세 가지 전제조건이 충족되어야 할 것이며, 특히 마지막 생리적 반응에 대한 거짓 여부 판정은 거짓말탐지기가 검사에 동의한 피검

- 상주 독극물 음료수 음독 살해사건의 경우 피의자의 거짓말 탐지기 검사결과가 허위진술로 나타남. 농약병 등에서 피의자의 지문이 나오지 않아 피의자의 혐의를 확신하지 못하던 여론의 분위기가 본 검사결과로 인해 반전되었음.⁵⁾ 현재 항소심에서 무기징역을 구형받아 대법원에 상고한 상태

□ 지능형 전자발찌

- 2008년 『특정 성폭력범죄자에 대한 위치추적 전자장치 부착에 관한 법률』에 의해 전자발찌 제도 시행. 이후 법의 개정으로 현재 성폭력 범죄뿐만 아니라 살인, 강도, 미성년자 유괴 범죄에도 부착 명령 가능
- 법무부 산하 보호관찰소의 보호관찰관이 업무 담당⁶⁾. 전자발찌 부착인원은 매년 늘어나 2015년 9월 기준 2167명이 전자발찌를 부착하고 있음⁷⁾
- 그러나 전자발찌를 차고 다시 범죄를 저지르거나 전자발찌를 끊고 도주하는 등 문제점이 지속적으로 나타나고 있음

사자의 생리적 반응을 정확히 측정할 수 있는 장치이어야 하고, 질문사항의 작성과 검사의 기술 및 방법이 합리적이어야 하며, 검사자가 탐지기의 측정내용을 객관성 있고 정확하게 판독할 능력을 갖춘 경우라야만 그 정확성을 확보할 수 있는 것이므로, 이상과 같은 여러 가지 요건이 충족되지 않는 한 거짓말탐지기 검사 결과에 대하여 형사소송법상 증거능력을 부여할 수는 없다.

(출처 : 대법원 2005.05.26. 선고 2005도130 판결[특정범죄가중처벌등에관한법률위반(도주차량)] > 종합법률정보 판례)

- 5) 티브이데일리 2015.8.7. 보도 “상주 농약 사이다 피의자 할머니 거짓말탐지기 결과 정확도 '의견 분분’” (<http://tvdaily.asiae.co.kr/read.php3?aid=1438940967957355016>)
- 6) 관련 기사: 경향신문 2013.9.9. 보도 “성남보호관찰소 이전반대” 학부모들, 집단 등교거부 움직임
- 7) NSP통신 2015.9.8. 보도 “전자발찌 부착자, 도입 이후 14배 증가한 2167명” (<http://www.nspna.com/news/?mode=view&newsid=140204>)

- 법무부는 2017년 말부터 맥박이 빨라지고 체온이 높아지는 등 범행 징후가 보이면 미리 대응할 수 있는 지능형 전자발찌를 운영할 계획⁸⁾

□ 뇌과학에 의한 범죄 가능성 예측

- 뇌가 보내는 신호나 뇌의 활성화 상태로 범죄 가능성을 예측하려는 시도



- 국내에서도 형사정책연구원에서 『뇌과학의 발전과 형법적 패러다임 전환에 관한 연구』등을 수행한 바 있어 이 분야에 대한 관심은 꾸준히 증가할 것으로 보임

8) 2015.1.21. 법무부 보도자료 “법질서 확립으로 국가혁신 기반을 마련하겠습니다” (http://www.moj.go.kr/HP/COM/bbs_03/ShowData.do?strNbodCd=noti0005&strWrtNo=3353&strAnsNo=A&strFilePath=moj/&strRtnURL=MOJ_30200000&strOrgGbnCd=100000); 법무부 범죄예방정책국 특정범죄자관리과 홍보자료 (http://www.moj.go.kr/HP/MOJ03/moj_40/moj_4080/moj_408010_popup.jsp) 참조

□ 생체신호는 생체정보(Bio Information)에는 포함
되지만, 생체인식(biometric)정보는 아님

- 따라서 생체신호는 지문, 홍채, 안면인식 등 생체인증을 접목한 사용자 인증 방식인 FIDO(Fast Identity Online)와는 관련성이 적음

Ⅲ. 수사 분야의 생체인식정보 활용 - CCTV 얼굴 인식

□ CCTV의 법적 근거 - 원칙적 금지, 예외적 허용

- 개인정보보호법 제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자

□ CCTV(closed circuit television, 폐쇄 회로 텔레비전)와 생체인식정보

- 특정 수신자를 대상으로 화상을 전송하는 시스템
- CCTV를 통해 알 수 있는 정보는 크게 안면(얼굴) 정보와 걸음걸이 정보
- 생체인식정보는 신체적 특성 정보와 행동적 특성 정보로 나뉘는데, 얼굴은 신체적 특성 정보이고 걸음걸이는 행동적 특성 정보임
- 지문이나 DNA정보와 달리 직접적 접촉 없이 정보를 수집할 수 있어 거부감을 줄일 수 있다는 장점 있으나, 현재까지는 조명, 얼굴 방향, 표정, 변장 등에 따라 식별률 낮아지는 단점 존재

□ CCTV 현황

- CCTV 설치는 매년 증가하고 있음. 2014년 기준 공공부문 CCTV는 65만대 정도였음. 공공부문 CCTV와 민간부문 CCTV를 합하여서는 560만대 정도로 추산됨(2015.10. 기준)
- ‘환경설계를 통한 범죄예방(CEPTED, Crime Prevention Through Environmental Design)’(약칭 셉테드)⁹⁾에서 CCTV를 적극 활용¹⁰⁾ 일

9) 경찰청훈령 『범죄예방진단 절차 및 활용에 관한 규칙』

제 2 조(정의) 이 규칙에서 사용하는 용어의 뜻은 다음과 같다.

1. “범죄예방진단”이란 경찰관이 지역사회와 함께 범죄예방대책을 마련하기 위해, 거리·공원·공공시설·건축물 등 특정 지역이나 시설의 물리적·사회적 환경 요인을 분석하여 범죄취약요소를 파악하는 활동을 말한다.
2. “범죄예방디자인”이란 건축물·시설·공간·제품 및 시스템 등에 있어 범죄예방 기능을 최적화시킨 설계·시설·기술 등을 말한다.

(<http://www.law.go.kr/admRulSc.do?menuId=1&query=%EB%B2%94%EC%A3%84%EC%98%88%EB%B0%A9#liBgcolor5>)

10) 국토교통부 『범죄예방 건축기준 고시』

반적으로 CCTV가 있다는 사실을 밝히는 것만으로도 어느 정도 범죄 예방 효과가 있다고 함¹¹⁾

- 범죄 현장을 찍은 CCTV가 있다고 하면 쉽게 자수하는 경향도 있음¹²⁾

제 4 조(접근통제의 기준) ① 보행로는 자연적 감시가 강화되도록 계획되어야 한다. 다만, 구역적 특성상 자연적 감시 기준을 적용하기 어려운 경우에는 폐쇄회로 텔레비전, 반사경 등 자연적 감시를 대체할 수 있는 시설을 설치하여야 한다.

제10조(아파트에 대한 기준)

③ 부대시설 및 복리시설은 다음 각 호와 같이 계획하여야 한다.

2. 어린이놀이터는 사람의 통행이 많은 곳이나 주동 출입구 주변이나 각 세대에 서 조망할 수 있는 곳에 배치하고, 주변에 경비실을 설치하거나 폐쇄회로 텔레비전을 설치하여야 한다.

④ 경비실 등은 다음 각 호와 같이 계획하여야 한다.

3. 경비실 또는 관리사무소에 고립지역을 상시 관망할 수 있는 폐쇄회로 텔레비전 시스템을 설치하여야 한다.

⑨ 승강기·복도 및 계단 등은 다음 각 호와 같이 계획하여야 한다.

1. 지하층(주차장과 연결된 경우에 한한다) 및 1층 승강장, 옥상 출입구, 승강기 내부에는 폐쇄회로 텔레비전을 설치하여야 한다.

2. 계단실에는 외부공간에서 자연적 감시가 가능하도록 창호를 설치하고, 계단실에 폐쇄회로 텔레비전을 1개소 이상 설치하여야 한다.

제13조(일용품 소매점에 대한 기준)

③ 출입구 및 카운터 주변에 폐쇄회로 텔레비전을 설치하여야 한다.

제14조(다중생활시설에 대한 기준)

② 건축물의 출입구에 폐쇄회로 텔레비전 시스템을 설치한다.

11) 김봉수, “범죄수사상 생체정보의 수집 및 활용에 대한 규범적 통제”, 전남대학교 법학논총 제35집 제2호, 264면.

12) 헤럴드POP 2015.1.31. “크림빵 빵소니 자수, “CCTV가 있다” 댓글이 범인 잡아”(http://pop.heraldcorp.com/view.php?ud=201501310014039617640_1&RURL=http%3A%2F2Fsearch.naver.com%2Fsearch.naver%3Fie%3Dutf8%26where%3Dnews%26query%3D%25EC%25B2%25AD%25EC%25A3%25BC%2B%25ED%2581%25AC%25EB%25A6%25BC%25EB%25B9%25B5%2BCCTV%2B%25EC%259E%2590%25EC%2588%2598%26sm%3Dtab_tmr%26firm%3Dmr%26sort%3D0%26url%3Dhttp%253A%252F%252Fbiz.heraldcorp.com%252Fview.php%253Fud%253D201501310014039617640_1%26ucs%3D7yhdvbW11LqS)

□ 범죄수사와 CCTV

- CCTV 분석에 의한 용의자 검거가 늘어남에 따라 2015년 4월부터 서울지방경찰청은 44명의 ‘CCTV 명인제도’를 운영. 범죄 수사가 주변 CCTV 분석으로 시작하는 경우가 대다수라고 함
- 경찰청에 따르면, CCTV 영상검색 고도화와 CCTV 신원확인 기술개선 등이 앞으로의 과제라고 함.¹³⁾ CCTV를 확인하는 작업도 엄청난 시간과 노력을 요하는 작업이기 때문에, 하나의 얼굴을 특정하면 다른 화면에서도 특정된 얼굴만을 추출해서 보여주는 기술도 등장
- 관제실에서 조종가능하고 움직임이나 비명을 감지할 수 있는 지능형 CCTV도 등장
- CCTV로 얼굴영역 검출 시 나머지 사람들 얼굴은 모자이크 처리하거나 스크램블링 처리하는 기술적 방안 등을 이용해 사생활침해 소지 줄일 수 있음
- 경찰청은 각 지자체에서 운영하는 CCTV통합관제센터와 연계해 영상 정보를 실시간으로 수집하는 시스템을 개발, 범죤자나 뺑소니범 검거 등에 활용하고 있었으나 국회에서 '개인정보보호법 정보주체 사전 동의 조항'에 위배 된다는 지적을 받아 해당 시스템 사용을 중단

13) 연합뉴스 2015.7.29. “<CCTV 수사> ① 모든 범죤 수사 출발점 되다”
(<http://www.yonhapnews.co.kr/bulletin/2015/07/28/0200000000AKR20150728173000004.HTML?input=1195m>)

IV. 수사 분야의 생체인식정보 활용 - CCTV 걸음걸이

□ 법보행

- 개인 식별이 어려울 때 사람의 걸음걸이를 분석해 동일인 여부를 판단하는 과학적 수사기법
- 원세훈 전 국정원장의 집에 화염병을 던진 혐의로 기소됐던 30대 회사원에 대해 CCTV 분석으로 영상에 찍힌 사람과 걸음걸이가 동일하다는 점을 증거로 제출하였으나, 법원에서 받아들여지지 않은 사례 있음(2014노1268). CCTV 동영상이 사본이었는데, 사본을 만드는 과정에서 저장장치가 봉인되지 않았음을 지적하며 원본과의 동일성, 무결성을 인정하지 않음
- 2016.1.23. 방영 ‘그것이 알고싶다 - 살인자의 걸음걸이’에서 CCTV에 나오는 걸음걸이를 분석하여 용의자를 특정하는 내용 방영. 영국에서는 2000년부터 법보행이 증거로 채택되었다고 함
- 걸음걸이의 특성에 대한 활용이 많아짐에 따라, 국가기술표준위원회에서는 5년마다 산출하는 인체지수에 걸음걸이 유형 입체영상을 추가하였음¹⁴⁾

14) 파이낸셜뉴스 2016.3.14. “인체지수 조사에 ‘걸음걸이’도 추가...범죄수사 및 장애인 환경 개선 기대” (<http://www.fnnews.com/news/201603141009535843>)

V. 수사 분야의 생체인식정보 활용 - 지문

□ 지문 데이터베이스

- 현재 지문 데이터베이스 운용 중(4억 개의 지문 수록). 2010년과 2012년에 지문 데이터베이스를 새로 입력하고 검색 프로그램인 지문검색시스템(Automated Fingerprint Identification System, AFIS)의 성능을 향상하였음. 가장 빠르고 편리한 신원 확인 방법으로 기능
- 경찰청은 2010년 이후 매년 살인·성폭력·강도·절도 등 공소시효가 남은 주요 미제 사건에 대해 지문 재검색을 실시. 지난해까지 5년간 총 3032개의 사건 관련 지문을 재검색해 1157명의 신원을 새로 확인. 덕분에 영구미제로 남은 뺨한 374건을 해결¹⁵⁾

□ 지문 채취에 대한 근거 법령

- 주민등록법 제24조(주민등록증의 발급 등) ②주민등록증에는 성명, 사진, 주민등록번호, 주소, 지문(指紋), 발행일, 주민등록기관을 수록한다.
- 검찰사건사무규칙 제15조(수사관계사항의 조회)
 - ② 검사가 사건을 인지하는 때에는 피의자의 지문을 채취하여 별지 제23호서식에 의한 수사자료표송부서에 의하여 지문대조조회를 하여야 하며, 범죄통계원표(발생사건표, 검거사건표, 피의자표)를 작성하여야 한다.
 - ③ 검사가 고소·고발을 받은 사건을 직접 수사하는 때에도 제2항과 같다. 다만, 고소·고발사건 중 다음 각호의 1에 해당하는 경우에는

15) 중앙일보 2015.7.11. “10초면 열 손가락 지문 파악 “척 보면 용의자 알아요”
(<http://news.joins.com/article/18217655>)

피의자가 「지문을 채취할 형사피의자의 범위에 관한 규칙」 제2조제2항제1호·제2호 또는 제4호의 1에 해당하지 아니하는 한 피의자에 대한 지문채취 및 지문대조조회를 하지 아니한다.

1. 혐의없음 2. 공소권없음 3. 죄가안됨 4. 각하 5. 참고인중지

④ 검사가 고소·고발사건 중 사법경찰관으로부터 지문을 채취하지 아니하고 제3항의 불기소의견, 참고인중지의견 또는 기소중지(피의자소재불명에 의한 경우에 한한다)의견으로 송치받은 사건이나 불기소처분에 대하여 재기수사·공소제기 또는 주문변경명령된 사건에 대하여 공소를 제기하거나 기소유예, 공소보류, 소년보호사건, 가정보호사건 또는 「성매매알선 등 행위의 처벌에 관한 법률」 제3장에 따른 보호사건(이하 "성매매보호사건"이라 한다) 송치의 결정을 하는 때에도 제2항의 규정에 의하여 피의자의 지문을 채취하여 별지 제23호서식에 의한 수사자료표송부서에 의하여 지문대조조회를 하여야 한다. 제2조제4호에 따라 송치받은 사건 및 같은 조 제11호에 따라 재정결정서를 송부받은 사건에 관하여도 또한 같다.

○ **경범죄 처벌법 제3조(경범죄의 종류)** ① 다음 각 호의 어느 하나에 해당하는 사람은 10만원 이하의 벌금, 구류 또는 과료(科料)의 형으로 처벌한다.

34. (지문채취 불응) 범죄 피의자로 입건된 사람의 신원을 지문조사 외의 다른 방법으로는 확인할 수 없어 경찰공무원이나 검사가 지문을 채취하려고 할 때에 정당한 이유 없이 이를 거부한 사람

○ **형의 집행 및 수용자의 처우에 관한 법률 제19조(사진촬영 등)** ① 소장은 신입자 및 다른 교정시설로부터 이송되어 온 사람에 대하여 다른 사람과의 식별을 위하여 필요한 한도에서 사진촬영, 지문채취, 수용자 번호지정, 그 밖에 대통령령으로 정하는 조치를 하여야 한다.

- **형의 실효 등에 관한 법률 제2조(정의)** 이 법에서 사용하는 용어의 뜻은 다음과 같다.

4. “수사자료표”란 수사기관이 피의자의 지문을 채취하고 피의자의 인적사항과 죄명 등을 기재한 표(전산입력되어 관리되거나 자기 테이프, 마이크로필름, 그 밖에 이와 유사한 매체에 기록·저장된 표를 포함한다)로서 경찰청에서 관리하는 것을 말한다.

□ 수사 과정에서 지문날인을 강제할 수 있는가?

- 헌법상 진술거부권은 인정되지만, 지문 등의 신체측정은 진술이 아니므로 진술거부권이 인정되지 않는다고 함¹⁶⁾
- 수사 기관에서 본인의 인적 사항 확인을 거부하며 진술거부권을 행사할 때, 신원 확인을 위해 지문 날인 강제하는 경우 있음
- 진술거부와 함께 지문 날인을 거부하는 경우, 진술은 강제할 수 없지만 지문은 영장을 받아 강제적으로 날인할 수 있다고 함

□ 지문+장문(손바닥에 난 손금의 무늬, hand geometry)

- 범행에 사용된 총기나 칼에 남은 지문과 장문을 함께 분석한다면 용의자 특정에 더욱 정확성이 높아지게 됨. 지문이 남은 범행 도구의 30% 정도에는 장문도 함께 남아있다고 함

16) 거짓말탐지기의 사용은 진술이라 볼 수 있으므로 진술거부권이 적용된다. 따라서 피의자가 거짓말탐지기의 사용에 동의하지 않으면 강제적으로 사용할 수 없다.

VI. 수사 분야의 생체인식정보 활용 - DNA

□ 디엔에이신원확인정보의 이용 및 보호에 관한 법률

- 제5조(수형인등으로부터의 디엔에이감식시료 채취) ① 검사는 ... 수형인등으로부터 디엔에이감식시료를 채취할 수 있다
- 제6조(구속피의자등으로부터의 디엔에이감식시료 채취) 검사 또는 사법경찰관은 구속된 피의자 보호구속된 치료감호대상자로부터 디엔에이감식시료를 채취할 수 있다.
- 제7조(범죄현장등으로부터의 디엔에이감식시료 채취) ① 검사 또는 사법경찰관은 다음 각 호의 어느 하나에 해당하는 것(이하 “범죄현장등”이라 한다)에서 디엔에이감식시료를 채취할 수 있다.
 - 1. 범죄현장에서 발견된 것
 - 2. 범죄의 피해자 신체의 내·외부에서 발견된 것
 - 3. 범죄의 피해자가 피해 당시 착용하거나 소지하고 있던 물건에서 발견된 것
 - 4. 범죄의 실행과 관련된 사람의 신체나 물건의 내·외부 또는 범죄의 실행과 관련한 장소에서 발견된 것② 제1항에 따라 채취한 디엔에이감식시료에서 얻은 디엔에이신원확인정보는 그 신원이 밝혀지지 아니한 것에 한정하여 데이터베이스에 수록할 수 있다.
- 제8조(디엔에이감식시료채취영장) ① 검사는 관할 지방법원 판사(군판사를 포함한다. 이하 같다)에게 청구하여 발부받은 영장에 의하여 제5조 또는 제6조에 따른 디엔에이감식시료의 채취대상자로부터 디엔에이감식시료를 채취할 수 있다.

- ② 사법경찰관은 검사에게 신청하여 검사의 청구로 관할 지방법원 판사가 발부한 영장에 의하여 제6조에 따른 디엔에이감식시료의 채취대상자로부터 디엔에이감식시료를 채취할 수 있다.
- ⑧ 디엔에이감식시료를 채취할 때에는 채취대상자에게 미리 디엔에이감식시료의 채취 이유, 채취할 시료의 종류 및 방법을 고지하여야 한다.
- 제9조 디엔에이감식시료의 채취 방법, 제10조 디엔에이신원확인정보의 수록 등, 제11조 디엔에이신원확인정보의 검색·회보, 제12조 디엔에이감식시료의 폐기, 제13조 디엔에이신원확인정보의 삭제, 제14조 디엔에이신원확인정보데이터베이스관리위원회, 제15조 업무목적 외 사용 등의 금지

□ 개인정보보호법 시행령

- 제18조(민감정보의 범위) 1. 유전자검사 등의 결과로 얻어진 유전 정보
- 개인정보보호법 제23조에서 ‘민감정보’의 예로 ‘건강에 관한 정보’를 들고 있는 것 외에 생체 정보를 법에서 정하고 있는 것은 위의 유전정보 뿐임
- 생체 정보는 단순히 개인정보인가? 아니면 더 나아가 민감정보나 고유식별정보인가? 에 대한 답은 앞으로 찾아가야 할 것으로 생각됨
- 행정자치부에서 운영하는 개인정보보호종합포털에서는 개인정보의 예시로 “신체정보 - 지문, 홍채, DNA, 신장, 가슴둘레 등”을 포함시키고 있음¹⁷⁾

17) <http://www.privacy.go.kr/nns/ntc/inf/personalInfo.do>

- DNA 정보 역시 FIDO(Fast Identity Online) 인증과는 관련이 적음

VII. 수사 분야의 생체인식정보 활용 - 성문(Voiceprint)

- 성문검사는 진술을 강요하는 것이 아니므로 진술거부권 적용되지 않는다고 함
- 보이즈피싱 사건에서 성문분석이 유용하게 쓰이고 있음

VIII. 해외 생체인식정보 범죄수사 활용 사례¹⁸⁾

- 미국 CIA 일급 보안 전산실에는 망막 스캔을 설치하여 부정 출입 통제
- 카지노에서 사기도박 전과자의 얼굴을 인식할 수 있는 카메라로 출입 관리
- 축구장에서 훌리건 등 폭력적인 축구팬들에 대한 출입 관리

18) 윤지영/이천현/최민영/민수홍/김재운/이원상, 『법과학을 적용한 형사사법의 선진화 방안(V)』, 한국형사정책연구원, 2014, 94면.

토 론 문

토 론 문

김 종 배
(서울디지털대 컴퓨터공학과 교수)

1. 생체정보의 정의

- Biometric Information or Data
- Information : 큰 범주(광의적), 미국 식, 활용에 중점
- Data : 작은 범주(지엽적), 유럽 식, 보호에 중점
- 국내는 Information 범주에 가까움 → 활성화에 중점을 둔 근거에 기초
- 다만, 생체정보의 영구불변성에 따른 보호 관점도 무시할 수 없음
- 이러한 관점에서는 생체정보는 이용자가 다 가지고 있어야 하고(보편 타당, 휴대, 비기억), 서로 달라야 하며(식별성), 시간·환경변화에 적은 영향을 가지는 정보(영구불변)일 것이다.

2. 생체정보의 범위

- 개인정보(고유식별정보, 민감정보)
- 수집하는 목적성 기준에 따른 다양한 범위

3. 생체정보 활성화 방안

- 주민번호가 있어 뛰어난 아용자 식별성을 가진다.
- 따라서 생체정보의 급속한 활용은 다소 디딜 수 있을 것이다.
- 그럼에도 생체정보의 활성화가 가능한 예측은 식별성과 더불어 편리함이다.

- 이러한 편리함에 있어 보호 측면이 가미되면서 보편타당한 서비스의 제공이 어려울 수 있다. (지문인식기, 카메라, 녹음기 등 추가적인 감지기 요구로)
- 현재 본인확인서비스의 경우 더 이상 이용자의 주민등록번호를 수집하고 있지 않기 때문에 점차적으로 해커 입장에서는 이용자의 주민등록번호로 비대면 온라인 거래(ex 온라인 쇼핑몰 등) 시 활용할 있는 기회가 줄어드는 것은 자명한 일일 것이다.
- 이러한 맥락으로 생체정보의 활성화 방안에는
 - ☞ 법 개정(의료법 등)을 통해 비식별화된 생체정보의 경우 동의 없이 사용 가능 방안 마련
 - ☞ 본인확인기관을 통한하여 생체정보인증으로 정보통신사업자 등이 생체정보를 활용한 서비스 제공에 추가 비용적인 부담을 줄이는 정책적인 방안 마련 필요 (생체정보 저장소는 필요하다. 다만, 일방향 암호화 등의 기술적 보호조치가 수단되어야 함)

4. 생체정보 보호 방안

- 생체정보 범주를 세부화 하여 서로 다른 보호 기준 적용 필요
- 민감한 정보를 포함하는 생체정보는 그렇지 않는 생체정보보다 엄격한 보호 기준 적용
- 중앙집중식 생체정보 저장소를 활용할 경우의 안전성과 위험성이 동시 상존함
- 현행 본인확인시스템의 보호 방안을 활용한 보호 모델 수립이 필요
 - ☞ 연계정보(=~주민번호2) = 일방향 암호화[주민등록번호 || 가입하고자 하는 웹사이트 식별번호 || 본인확인기관 비밀키
 - ☞ 연계정보(=~주민번호2) = 일방향 암호화[주민등록번호 || 가입하고자 하는 웹사이트 식별번호 || 본인확인기관 비밀키 || 생체인식정보]

- ☞ 생체인식정보 = 일방향 암호화[지문정보 || 주민등록번호]
- 해커의 공격 포인트는 암호화된 데이터가 아니라 암호화 하는 키 저장소이다. 따라서 생체정보 암호화는 하드웨어 암호화 방식을 적용하고 데이터와 암호화 키의 물리적인 분리 저장
- 이러한 기술적 보호조치는 기존 개인정보보호 법령과 다른 법규 제정이 필요

제4차 워크숍
주요 외국의 생체정보 관련
법제 동향

2016. 6. 27.

일 정

1. 목 적 : 주요 외국의 생체정보 관련 법제 동향
2. 일 시 : 2016년 6월 27일(월) 09:00~15:00
3. 장 소 : 서울역회의실 2호실
4. 세부일정
 - (1) 사 회
 - 김일환(성균관대 법전원 교수)
 - (2) 연구개요 발표
 - 김현희(연구책임, 한국법제연구원 연구위원)
 - (3) 발 표
 - 독일의 생체정보 관련 법제 동향
: 김영미(사회자본연구원 연구원)
 - 프랑스의 생체정보 관련 법제 동향
: 오승규(중원대 법학과 교수)
 - 미국의 생체정보 관련 법제 동향
: 이상경(서울시립대 법전원 교수)
 - 일본의 생체정보 관련 법제 동향
: 강영기(고려대 법학과 연구교수)
 - (4) 토 론
 - 김현경(서울과기대 IT정책전문대학원 교수)
 - 손형섭(경성대 법학과 교수)
 - 윤석진(강남대 법학과 교수)
 - 정필운(한국교원대 일반사회교육과 교수)
 - 최경환(한국인터넷진흥원 책임연구원)
 - 황현영(국회 입법조사처 입법조사관)

목 차

□ 발 제 문	175
○ 독일의 생체정보 관련 법제 동향(김영미)	177
○ 프랑스의 생체정보 관련 법제 동향(오승규)	189
○ 미국의 생체정보 관련 법제 동향(이상경)	199
○ 일본의 생체정보 관련 법제 동향(강영기)	225
□ 토 론 문	237
○ 토론문(손형섭)	239

발 제 문

독일의 생체정보 관련 법제 동향

김 영 미
(사회자본연구원 연구원)

I. 들어가며

- 독일에서 생체정보는 “Biometrie” 또는 “Biometrische Daten”이란 표현으로 사용됨.
 - 생체정보는 다른 개인정보와 달리 변경할 수 없는 사람의 신체적, 행동적 고유한 특성을 가지는 개인의 신원확인 정보를 의미함.
- 이러한 생체정보에 관한 논의는 생체인식기술과 컴퓨터시스템의 발달과 함께 개인정보보호와 관련한 문제와 직결됨.
- 현재 독일에서 생체정보는 주로 공적분야에서 개인의 신분확인을 위해 여권, 체류허가 및 기타 신분증에 저장하여 활용하고 있으며, 특히 2005년 11월부터 지문 등의 생체정보 칩을 저장한 전자여권을 사용하기 시작하면서, 생체정보의 활용과 개인정보의 침해 및 보호의 문제가 대두됨.
- 따라서 현행 독일법제상 생체정보의 활용과 보호 사이에서 국가의 개입이 어떻게 이루어지고 있는지를 살펴보는 것은 우리의 생체정보관련 법제의 정비방향을 설정하는데 도움이 될 것으로 생각된다.

II. 생체정보 관련 법제

1. 테러방지법

- 2001년 9·11 테러가 난 이후, 독일은 유럽연합이 테러행위에 대한 공동대처를 결정하는데 앞서 이미 신분증명에 대한 각종 법률을 개정하여 생체정보를 활용하기 시작함.

- 근거가 되는 법이 2002년 1월 9일 전면 개정된 「국제적인 테러리즘의 방지를 위한 법률(Gesetz zur Bekämpfung des internationalen Terrorismus, Terrorismusbekämpfungsgesetz, TBG)」, 즉 테러방지법임.
- 21개의 조항과 시행령으로 구성된 테러방지법은 여권 및 개인신분증, 외국인을 위한 증명서류에 생체정보를 저장하는 것과 관련한 규정을 주요 내용으로 하고 있다.
- 이를 통해 여권법과 개인신분증명법상의 생체정보의 저장과 관련한 내용을 개정하였으며, 외국인체류법(AufenthG)과 난민법(AsylG) 규정을 통해서도 외국인과 난민신청자들의 신분증에도 생체정보의 저장이 요구되었다. 물론 이러한 생체정보에 관한 규정은 내용상 적정성, 필요성과 적절성을 전제로 한다.

1) 여권법(PassG)

- Verordnung (EG) Nr. 2252/2004을 근거로 한 테러방지법 제7조에 의해 여권법 제4조에 2개의 추가조항이 신설되었다.
- 제4조 제3항과 제4항에서 사진과 서명 이외에 지문 또는 용모와 같은 생체정보를 저장할 수 있고, 여권에 사진, 서명 및 기타 생체정보는 보안상 암호화된 형태로 저장할 수 있다고 규정하고 있음
- 생체정보의 종류, 세목과 암호화된 형태로 표시 및 저장, 저장형태, 기타 가공 및 이용에 관해 연방법률에서 규정함.
- 아울러 개인의 일반정보 외에 여권에 저장되는 생체정보로 사진, 특정 손가락의 지문, 지문 납입상태에 관한 규정을 두고 있으며, 권한 없이 해당 정보를 열람, 변경 및 삭제할 수 없고, 생체정보를 저장하는 은행의 설립은 하지 않는다고 명시하고 있다(동법 제4조 제3항).
- 이러한 생체정보의 활용은 기본권을 침해하지 않아야 하고, 행정청에 한하여 수집할 수 있으며, 작업 및 이용권한은 관련 행정청이 가지도록 하고 있다(제22조).

2) 개인신분증명법(PAuswG)

- 독일의 개인신분증명은 「개인신분증 및 전자신원증명에 관한 법률 (Gesetz über Personalausweise und den elektronischen Identitätsnachweis, PAuswG)」에 근거하며, 생체정보의 저장은 2002년 1월 9일부터 허용함.
- 구체적인 사항은 동법 시행령(Personalausweisverordnung, PAuswV)과 수수료 관련 시행령(Personalausweisgebührenverordnung, PAuswGebV)에서 규정함.
 - 2010년 개정으로 전자 개인신분증 관련 규정이 다수 포함되었고, 보안으로 신분증을 맡기거나 포기할 필요가 없음(동법 제1조 제1항 제1문).
 - 또한 신분증 소지자는 자신의 비밀번호가 남용되지 않도록 보호할 책임을 부담한다(제27조 제2항).¹⁾ 저장되는 생체정보에는 사진과 지문이 있으며, 지문은 당사자의 신청이 있는 경우에만 저장할 수 있다(제5조 제9항).
- 이러한 생체정보에 대해서는 행정청이 수집, 열람, 비교할 수 있는 권한을 가진다(제17조).

3) 외국인체류법(Aufenthaltsgesetz, AufenthG)

- 독일은 「외국인의 독일내 체류, 소득활동 및 이민에 관한 법률 (Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet, AufenthG)」, 즉 외국인체류법을 통해 외국인의 신분증명, 즉 체류허가증에 생체정보를 저장할 수 있음.

1) § 27 (Pflichten des Ausweisinhabers)

(2) Der Personalausweisinhaber hat zumutbare Maßnahmen zu treffen, damit keine andere Person Kenntnis von der Geheimnummer erlangt. Die Geheimnummer darf insbesondere nicht auf dem Personalausweis vermerkt oder in anderer Weise zusammen mit diesem aufbewahrt werden. Ist dem Personalausweisinhaber bekannt, dass die Geheimnummer Dritten zur Kenntnis gelangt ist, soll er diese unverzüglich ändern oder die Funktion des elektronischen Identitätsnachweises ausschalten lassen.

- 외국인의 신원확인에 활용되는 생체정보는 사진과 지문으로 제한함.
- 동 법은 연방내무부에 외국인, 난민, 무국적자의 여행자증명에 관한 권한을 부여하였으며, 규칙을 제정하여 생체정보의 수집, 분류, 저장, 및 삭제 등의 절차와 기술적 사항을 규정함.
- 이에 따라 집행권한을 위임받은 행정청이 저장된 생체정보를 열람하는 것과 당사자로부터 필요한 생체정보의 수집 및 상호 비교할 수 있는 권한을 가진다(제49조 제1항 제1문).

4) 난민법(AsylG)

- 독일의 난민절차법(AsylVfG) 2015년 10월 24일부터 난민법(AsylG)으로 명칭을 변경하여 적용되고 있음.
- 동법은 기본법 제16조 난민권을 실현하기 위한 법률로서 외국인 체류법과 더불어 난민에 대한 기본적인 규범을 형성함.
- 독일 연방정부는 연방참사원의 동의를 받아 난민에 대해서는 생체정보의 범위를 일반 외국인 등록의 경우와 다르게 정할 수 있음.
- 외국인체류법과 달리 난민법에서는 행정청이 수집, 열람할 수 있는 생체정보의 범위를 사진과 지문외에 홍채까지 확대하였음(제16조 제1항의a).

5) 전자서명기본법

- 독일의 서명법은 2001년 5월 16일 제정된 「전자서명기본법(Gesetz über Rahmenbedingungen für elektronische Signaturen, SigG)」에 의하여 폐지됨.
- 2004년 개정된 전자서명기본법에서는 유효한 서명에 인증을 필수요건으로 하였는데(동법 제2조 제9호), 이는 전자서명 기술의 진보로 생체서명시스템 공급자가 신원확인에 자필서명을 사용할 수 있도록 한 것임.

- 「전자서명시행령(Verordnung zur elektronischen Signatur, SigV)」 15조 제1항에서는 「전자서명기본법」 제17조 제1항 제1문에 따라 안전한 서명을 위해 복수의 생체정보를 사용할 수 있도록 보장함.

Ⅲ. 개인정보의 침해와 보호

1. 유럽 개인정보보호 기본규칙

- 개인정보의 활용시 개인의 보호와 자유로운 정보교류를 위한 1995.10.24. 지침 95/46 (Richtlinie 95/46/EG) 제2조에 의하면, 개인정보는 특정인 또는 특정 가능한 사람(당사자)에 관한 모든 정보를 의미함.
 - 특히 색인번호나 신체적, 정신적, 심리적, 경제적, 문화적 또는 사회적 동일성을 표현하는 하나 혹은 다수의 특유한 요소에 의해 직접 또는 간접적으로 동일시 될 수 있는 사람은 특정 가능한 것으로 봄.
 - 개인정보의 활용은 자동적인 절차 또는 그와 관련하여 수행되는 각각의 과정, 즉 수집, 저장, 조직, 보존, 조정 혹은 변경, 선택, 시험, 이용, 전달에 의해 이전, 확장 또는 기타 다른 형태의 공급, 결합 또는 연결 및 차단, 삭제 또는 제거와 같은 개인정보와 관련한 일련의 모든 과정에서 이루어짐.
- 2016년 4월 27일 새롭게 정립된 유럽 영역 내의 ‘정보보호 기본규칙’, 즉 “개인정보 취급시 자연인 보호와 자유로운 정보 교환 및 Richtlinie 95/46/EG의 폐지를 위한 유럽 규칙(Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie

95/46/EG, Datenschutz-Grundverordnung)”에서 생체정보의 활용에 대한 내용이 포함됨.

- 유럽연합의 ‘정보보호 기본규칙’은 회원국에 직접 적용되며, 독일 내 별도의 법률 제정 없이 생체정보를 포함한 개인정보 취급에 대해 직접적인 구속력을 가짐.
 - 동 규칙에서 정하는 ‘정보보호 기본원칙’은 기존의 ‘허가유보부의 일반적 금지’, ‘정보최소화의 원칙’, ‘합목적성 및 투명성 원칙’을 그대로 유지·발전시킴.
- 이행지법주의(Marktortprinzip)에 따라서 적용 범위를 “유럽 시장”으로 확대함.
 - 유럽연합 내에 근거를 두고 있는 기업은 물론 유럽연합 밖에 있는 기업도 그 상품이 유럽 연합 내의 특정 국내 시장을 목표로 하거나, 개인정보의 처리가 유럽연합 내에 있는 사람의 행동에 관한 것일 경우에는 적용범위에 포함시킴.
- 유럽연합내 통일적 법적용을 위한 정보취급 조치를 도입함.
 - 다수의 회원국에서 영업활동을 하는 기업의 경우 원칙적으로 각 지역의 정보보호 감독청 사이에 합의와 협력을 통해 감독 업무를 수행하고, 본사에 감독청의 결정 내용을 송부하는 방식 적용(이른바 “One-Stop-Shop” 메커니즘).
 - 정보보호 기본규칙은 개별 행정청 사이에 합의가 이루어지지 않을 경우, “협력 절차(Kohärenzverfahren)”에 따라 각 행정청이 유럽 정보보호위원회의 결정에 근거하여 개별적으로 결정을 내릴 수 있음.

2. 독일 개인정보보호법

- 생체정보는 개인의 신체적인 정보와 직접 연관된다는 점에서 엄격히 보호되어야 할 민감한 정보를 포함할 수 있음. 이러한 개인정보

보의 보호는 ‘정보자기결정권’과 관련되며, ‘특히 민감한 정보’에 대해서는 특별한 취급조건을 따르도록 하고 있음(유럽 정보보호 기본규칙 제9조 참조).

□ 개인정보 보호와 관련해서는 “연방정보보호법(Bundesdatenschutzgesetz, BDSG)”이 기본적인 근거규범이 됨.

- 남용여부와 관계없이 조사에서 저장, 사용, 전달에 관하여 규정함. 단순한 정보남용에서 개인을 보호하는 것에 국한되지 않음.
- 연방정보보호법은 정보자기결정권 보호를 위해 목적구속원칙을 엄격히 적용하고 있음. 과제수행을 위해 필요하고 처리목적에 부합하는 조사, 저장, 변경, 이용 등을 허용함.²⁾

□ 생체정보의 수집, 처리를 위해서는 특별한 법적 근거를 필요로 하며, 특별법이 없으면 연방개인정보보호법에 의하여 처리함.

- 형사소송법 제161조 제1항 제1문에서 형사소추와 관련하여 모든 관청에 생체인식정보를 요구할 수 있는 권한만 인정됨.
- 형사소송법 제98조의a에 의해 중대한 범죄행위가 있었다고 할 만한 충분한 단서가 있는 경우 비공공기관이 보유하는 생체인식 정보에 접근할 수 있음.
- 형사소송법 제98조의b에 의해 법관의 명령이 있으면 다른 정보와 비교하여 일정한 특징을 가진 사람의 정보를 확인할 수 있음.
- 단체협약, 경영합의와 관련하여 생체정보의 처리가 가능함. 특히, 경영조직법(Betriebsverfassungsgesetz)과 연방직원대표법(Bundespersönalvertretungsgesetz)에 따른 공동결정권에 근거하여 경영협의회나 인사 협의회를 통해 근로자 감독시스템을 도입할 수 있음.³⁾

□ 연방정보보호법의 주요조항

- § 3 Weitere Begriffsbestimmungen (기타 개념정의)

2) 김일환, 12면.

3) 김일환, 19면.

- § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (정보수집, 처리, 이용허가)
- § 4a Einwilligung (동의)
- § 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (광학적·전자적 설비에 의한 공개적인 접근공간에 대한 감시)
- § 22 Wahl und Unabhängigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (연방정보보호청의 선택 및 독립)
- § 28 Datenerhebung und -speicherung für eigene Geschäftszwecke (고유한 사업목적을 위한 정보수집 및 저장)

IV. 판례동향

1. 개 관

- 개인 정보의 수집과 활용은 당사자의 동의가 있거나 법률의 규정이 있을 경우에만 허용됨.
- 연방정보보호청(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI)에 의하면, 생체정보를 포함한 개인 정보의 활용은
 - 당사자가 동의한 계약을 실행하기 위해서 또는 당사자의 신청에 따라 이루어진 계약의 선행 조치를 위해 필요한 경우,
 - 법적 의무 이행을 위해 필요한 경우,
 - 당사자 또는 다른 사람의 생존에 중요한 이익을 보호하는데 필요한 경우,
 - 공공의 이익 또는 공적인 과제 수행을 위해 필요한 경우,
 - 의무자 또는 제3자의 정당한 이익을 보장하기 위해 필요하지만,

당사자의 이익 또는 기본권 및 기본적인 자유를 침해하지 않는 경우⁴⁾에 가능함.

- 독일에서는 유럽법이 요구하고 있는 기준에 따라 위에서 언급한 법률들을 근거로 생체정보를 수집하고 있음.
- 이와 관련하여 연방법원, 연방헌법재판소 및 유럽 법원의 판결을 살펴볼 필요가 있음.

2. 독일 법원의 판례

- 독일 내에서 생체정보 활용을 허용할 것인가를 전면적으로 다른 판례는 아직까지는 찾아볼 수 없고, 연방헌재가 생체정보의 사용이 기본법에 위반하는지 여부도 판단한 바 없음.
- 다만, 현재는 2012년 12월 30일 여행자여권에 생체정보를 저장하는 것이 허용되는지에 대한 헌법소원을 각하한 바 있음.⁵⁾
 - 이 결정에 의하면, 전자적 방식으로 저장된 생체정보가 정보은행 형식으로 저장되고 수사 등의 목적으로 이용된다면 기본법상의 정보적 자기결정권을 침해할 가능성이 있다고 헌법소원을 제기하였으나 구체적으로 어떤 조치나 법규정이 권리를 침해하고 있는지 적시하지 않아서 각하됨.

3. 유럽 법원의 판결

- 독일의 여권법 제4조 제3항은 회원국가에서 발급된 여권과 여행증명서의 생체정보와 보안성 규범인 유럽규칙 VO(EG) Nr. 2252/2004에 상응하는 규정임

4) 다만, 행정청에 대해서는 적용되지 않음(BfDI, Datenschutz-Grundverordnung, 2016. 5, S. 10).

5) BVerfG, Beschluss vom 30. 12. 2012 - 1 BvR 502/09 = BeckRS 2013, 47059.

- 여권과 다른 여행증명서의 안전이라는 관점에서 여권에 대한 최소보장규범으로 도입됨.
- 이에 따라 행정청이 시민의 지문을 수집·저장할 수 있음.
- 2013년 유럽법원 판결에 의하면, 독일 시민 미하엘 슈바르츠(Michael Schwarz)가 게젤키르헨 행정법원(VG Gelsenkirchen)에 유럽 인권협약(EU-Grundrechtecharta) 제7조와 제8조 제1항에 근거하여 독일 여권법과 유럽법 규정에 의문을 제기하였고, 동 법원은 유럽법원에 그 판단을 의뢰하였고, 유럽법원이 제시한 정당화 사유는 다음과 같음.⁶⁾
 - 손가락 지문의 수집과 저장이 개인정보 보호의 관점에서 개인의 권리를 일부 침해한다고 인정할 수 있으나, 여권 내지 여행자 서류 오남용에 대비할 필요가 있음.
 - 이 관례에서 지문 수집의 필요성은 여권이나 여행자 서류를 타인이 이용하는 것을 방지하여 공공의 이익을 추구한다는 목적에 기인한다는 점에서 유럽인권협약의 취지에 부합함.
 - 개인정보 보호는 ‘비례성(Verhältnismäßigkeit)’에 따라 판단되어야 함으로 지문의 저장이 오남용을 완전히 방지할 수는 없지만, ‘현저히 경감’ 시킬 수는 있고, 현재로서는 지문의 수집 외에 다른 대안이 사실상 존재하지 않음.
 - 특히, 홍채 인식은 아직은 기술 및 비용적 측면에서 불가능한 상황임.
 - 수집된 지문 정보의 오남용 방지를 위한 보호 장치가 충분히 되어 있음
- 그러나 이상의 정당화 사유 외에 다른 생체정보에 대한 저장 및 취급 요건에 대하여 언급하지 않았고, 게젤키르헨 행정법원(VG Gelsenkirchen)이 유럽법원에 판단을 의뢰 하면서 제기했던 중앙시스템에 저장하는 문제와 수집한 생체정보를 다른 목적을 위해 사용할

6) EuGH, Urt. v. 17. 10. 2013 - C-291/12 = NVwZ 2014, 435.

수 있는 위험성에 대해서 언급하지 않아 판단을 회피하였다는 비판을 받고 있음.⁷⁾

- 2015년의 판결에서도 네덜란드의 국내법이 유럽법에 따라 여권에 지문 정보를 저장하도록 한 규정이 유효하다는 유럽법원의 판결이 있었음.
- 특히 각 회원국들이 여권에 활용하기 위해 수집·저장한 생체정보를 다른 목적으로 사용하지 않을 것이라는 점을 국내법 규정을 통하여 보장할 의무는 없다고 판단하였음.⁸⁾
- 마찬가지로 개인정보 보호 관점의 법적 판단을 회피하였다는 비판을 받음.⁹⁾

V. 나오며

- 사람의 고유한 신체적, 행동적 특징을 이용하여 개인의 신원을 확인하는 지문, 서명, 얼굴, 홍채 등의 생체정보는 그 자체가 직접 개인을 나타내기 때문에 보호의 문제가 특히 중요함. 여권, 여행자 증명서 등에서 생체인식기술이 구체화되고, 전자상거래가 활성화되면서 생체정보의 활용 문제가 더욱 중요시 됨. 따라서 생체정보에 관한 문제를 개인정보의 침해 뿐 아니라 법제적 차원에서 활용과 보호를 동시에 고려할 필요가 있음.
- 생체정보의 활용과 보호에 관한 독일의 입법은 유럽규정이 나오기 전에 이미 이루어졌고, 개별적인 법률에서 생체정보의 수집 및 처리에 대해 규정하고 있음. 독일의 생체정보에 관한 법률은 아직은 제한적으로 규정하고 있으나, 점진적으로 확대되고 있는 경향을

7) Pfeiffenbring, EuGH: Erfassung von Fingerabdrücken in Reisedokumenten, MMR-Aktuell 2013, 352719.

8) EuGH, Urt. v. 16. 4. 2015 - C-446/12 bis C-449/12 = BeckEuRS 2015, 431545.

9) Biselli, Urteil des Europäischen Gerichtshofes zu biometrischen Personalausweisen ignoriert Datenschutz, Netzpolitik, 21. 4. 2015.

찾아볼 수 있음. 유럽법원의 판결과 독일내 판례 모두 여권에 생체정보를 저장하는 문제에 대해 정당성을 인정하는 경향을 보이며, 완벽하진 않지만 법률상 보호수단을 통해 충분히 보호될 수 있다는 입장에 있음.

< 참고문헌 >

김일환, 독일의 생체정보보호법제에 관한 연구, 성균관법학 제18권 제1호, 2006.6.

ARIKEL-29-DATENSCHUTZGRUPPE, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, 27. April 2012.

http://ec.europa.eu/justice/data-protection/index_de.htm

BfDI, Datenschutz-Grundverordnung, BfDI-Info 6, 2. Auflage, Mai 2016.

Biselli, Anna, Urteil des Europäischen Gerichtshofes zu biometrischen Personalausweisen ignoriert Datenschutz, Netzpolitik, 21. 4. 2015
<https://netzpolitik.org/2015/urteil-des-europaeischen-gerichtshofes-zu-biometrischen-personalausweisen-ignoriert-datenschutz/>

Gothaer Versicherungsbank (Hrsg.), Biometrische Risiken 2014, F.A.Z - INSTITUT, April 2014.

Pfeiffenbring, Julia, EuGH: Erfassung von Fingerabdrücken in Reisedokumenten, MMR-Aktuell 2013, 352719.

Petermann, Thomas/Sauter, Arnold, Biometrische Identifikationssysteme, TAB Arbeitsbericht Nr. 76, Februar 2002.

TELE TRUST Deutschland e.V., White Paper zum Datenschutz in der Biometrie, 11.03.2008.

프랑스의 생체정보 관련 법제 동향

오 승 규
(중원대학교 법무법학과 교수)

I. 시작하며

생체정보(données biométriques)는 생체인식으로부터 도출된 정보를 말한다. 생체인식(biométrie)은 본래 측정(mesure)과 생물(vivant)의 합성어로서 생물을 측정한다는 의미에서 출발하여 오늘날 농학(agronomie), 인류학(anthropologie), 생태학(écologie), 의학(médecine) 등 광범위한 분야에서 수행되는 ‘생물에 대한 양적 연구(étude quantitative des êtres vivants)’를 가리킨다.¹⁾ 즉 통계학을 이용한 생물연구라고 할 수 있겠다. 이 생체인식은 본래의 학문적 의미로서의 생물통계학(biostatistique) 외에도 점점 그 사용목적의 의미를 인증(authentication)이나 신원확인(identification)의 의미로 사용되는 경우가 늘어나게 되었다. 20세기에 들어와서는 더 구체적으로 지문, 얼굴의 특징 등과 같은 ‘생물학적 특성(charactéristiques biologiques)’을 이용하여 사람의 신원을 확인한다는 의미로 명확히 사용되기 시작하였다. 정보통신기술의 발달에 따라서 생체인식 기술은 ‘보안 분야(domaine de la sécurité)’에서 접근을 통제하는 시스템에 적용되어 하나의 보안시스템 자체를 지칭하는 ‘생체인식통제 시스템(système de contrôle biométrique)’이라는 용어로도 사용되기에 이르렀다. 신원확인을 하는 데 쓰여지는 생체정보로는 지문(empreintes digitales), 홍채(iris), 손가락과 발가락의 정맥총(réseaux veineux), 손의 형태(morphologie de la main), 얼굴윤곽(traits du visage) 등이 있다. 타이핑 방식, 음성, 서명 방식 등을 대상으로 하는 행동분석(analyse com-

1) <https://fr.wikipedia.org/wiki/Biom%C3%A9trie>. 2016년 6월 10일 방문.

portementale)에 의해 나온 결과를 생체인식의 요소로 보기도 한다. 보안이라는 목적을 달성하기 위하여 사람의 생체정보를 이용한다는 점에서 윤리적 문제를 야기하게 되고 이것은 법적 문제로까지 이어진다. 특히 정보화시스템을 이용한 생체인식은 사생활 침해의 위험성을 항상 내포하고 있다.

생체인식은 “한사람의 체격과 생체적 특성 그리고 행동상의 특징으로부터 그를 자동적으로 확인하기 위한 정보기술의 총체”를 결집한다.²⁾ 생체정보는 한 개인을 특정할 수 있게 해준다는 점에서 개인정보로서의 성격을 가진다고 할 수 있고, 유전자나 지문의 예에서 보듯이 유일(unique)하고 영속적(permanent)인 특성을 띠고 있다. 이러한 생체정보를 통해 개인의 이력(traçage)을 파악하는 것이 가능한데, 이는 곧 기본권 침해의 우려를 불러일으키고 있다. “생체인식기술의 불가피한 발전과 나노테크놀로지 시대에 직면하여, 개인과 법률가들의 각성과 실천의지가 지금 당장 절대적으로 필요하다. 20년 후면 이미 너무 늦으리라.”³⁾는 Alex Türk의 말은 생체인식의 발전에 내제한 기본권 관련 법적 문제점을 잘 표현하고 있다. 생체인식은 기술에 대한 최고의 권리와 보안에 대한 강력한 요구가 맞물리면서 비약적으로 발전해왔다.⁴⁾ 반면, 생체인식은 정보보호와 사생활존중에 대한 개인의 권리와 안전에 대한 단체적 요구를 대치시키고 있기 때문에 권리와 공익 간의 균형을 모색해야만 한다.⁵⁾ 그러나 이 분야에 관한 특수한 법리가 아직은 확립되지 않았기 때문에, 특히 학교나 기업 또는 안전 부문에서 기본

2) David FORREST, Droit des données personnelles, Galiano, 2011.

3) Alex TÜRK, Propos tenus lors de la Conférence du 22 novembre 2011 à la Faculté Alexis de Tocqueville - DOUAI.

4) Ayse CEYHAN, « La biométrie : une technologie pour gérer les incertitudes de la modernité contemporaine. Applications américaine », Cahier de la sécurité, 56, 61-89, 2005.

5) Christian BYK, « Biométrie et Constitution : est-il trop tard pour les libertés publiques ? », La semaine juridique, Éd. Générale, 25, 19-22, 2008.

권에 대한 ‘해로운 불균형상태(déséquilibre préjudiciable)’에 처해 있는 실정이다. 한번 통신망에 올라간 개인의 생체정보는 계속 추적가능한 이력을 남기고 누구나 그것을 취득하여 이용할 수 있게 됨으로써 개인의 사생활이 추적되는 세상이 되고 말았다.⁶⁾ 이러한 현상에 대처하기 위해 국내법은 물론이고 유럽 차원의 국제법적 노력이 계속되고 있다. 정보의 보호를 위한 그룹 프로젝트인 G29⁷⁾가 대표적이다.

II. 프랑스에서 생체인식에 관한 법 현상

프랑스에서의 생체인식에 대한 의미는 교육적(pédagogique), 정치적(politique), 미디어적(médiatique), 사법적(judiciaire), 경제적(économique), 기술적(technologique) 의미 등으로 다양하게 사용되고 있다.⁸⁾ 그를 둘러싼 법적 논의를 살펴보기로 한다.

사전적으로는 “특정 군 내부의 생물다양성을 수학의 도움을 받아 연구하는 학문”으로 정의⁹⁾되고 있는 생체인식(biométrie)은 현실에서는 특정인의 신체상의 혹은 행동상의 특성에 기초하여 그 사람을 자동적으로 인식하게 함으로써 사람의 신원을 확인하는 것을 가능하게 해준다. 형사사건에서 범인을 특정하기 위해 사용되었던 것이 이제는 민사와 행정 분야에도 널리 사용되고, 국제법적으로도 특히 생체정보를 담은 여권의 사용을 둘러싼 논의가 있다.

6) Frédéric OCQUETEAU & Daniel VENTRE, « Problèmes politiques et sociaux », Éd. Documentation française, n° 988/sept. 2011.

7) Article 29 de la directive 95/45/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à la traitement de données à caractère personnel et à la libre circulation des données.

8) Pierre LECLERCQ, « À propos de la biométrie . - (Quelques réflexions après visite de l'exposition « Biométrie, le corps identité » à la Cité des sciences) », Communication Commerce électronique n° 3, Mars 2006, étude 7.

9) Petit Robert.

1. 인적 특성 정보의 처리

개인적 특성이 담긴 정보를 ‘처리(traitement)’한다는 것은 법률 제 78-17호인 소위 ‘정보문서자유법’ 제2조 제3항에서 “그 절차에도 불구하고 이러한 정보에 관한 모든 작용 또는 작용들의 총체”를 포괄하는 것으로 정의하고 있다. 동일 조항에서는 계속하여 “수집, 저장, 조직, 보존, 검색, 개조, 발췌, 조회, 사용, 전달에 의한 전파, 배포나 다른 형태의 처분, 상호접근 또는 교차, 잠금, 제거나 파기”를 예시하고 있다. 용어를 축적하는 것은 ‘처리’라는 낱말에 넓은 의미를 부여하려는 의지를 보여주는 것¹⁰⁾이라고 볼 수 있다. 판례를 통해서도 개념이 확장되고 있다. 비록 파일에 저장은 하지 않더라도 광고를 발송하기 위해 이메일 주소를 확인하는 것¹¹⁾, 전화안내를 목적으로 다른 기업의 가입자들의 개인적 특성이 담긴 자료를 전달하는 것¹²⁾, 보건당국에 전달할 목적으로 구국민건강법전 제11조에 규정된 질병에 관련된 개인들의 정보를 수집하는 행위¹³⁾ 역시 여기에 해당한다. 여권발급을 위해 지문을 채취하고 보존하는 것¹⁴⁾과 외국인등록의 차원에서 외국인의 생체정보를 수

10) J. Frayssinet, La protection des données personnelles, in A. Lucas, J. Devèze et J. Frayssinet, Droit de l'informatique et de l'internet : PUF, 2001, n° 122.

11) Cass. crim., 14 mars 2006, n° 05-83.423, F - P + F c/ Min. publ. : JurisData n° 2006-032892 ; Bull. crim. 2006, n° 69 ; Rev. Lamy dr. immat. 2006, n° 16, 471, note J. Le Clainche ; Rev. Lamy dr. immat. 2006, n° 17, 498, note P. Belloir ; D. 2006, p. 1066 ; JCP G 2006, IV, n° 1819 ; Comm. com. électr. 2006, comm. 131, A. Lepage.

12) CJUE, 5 mai 2011, aff. C-543/09, Deutsche Telekom, point 53 : Europe 2011, comm. 268, L. Idot.

13) CE, ass., 30 juin 2000, n° 210412, Ligue des droits de l'homme et du citoyen : JurisData n° 2000-060767 ; AJDA 2000, n° 10, concl. P. Fombeur ; JCP G 2000, IV, n° 46, 2742 ; LPA 13 févr. 2001, n° 31, p. 10, note R. Diane ; Gaz. Pal. 10 mars 2001, n° 69, p. 21, obs. P. Graveleau ; Gaz. Pal. 17 juill. 2001, n° 198, p. 42, note A.-F. Godet.

14) CE, ass., 26 oct. 2011, n° 317827, Assoc. pour la promotion de l'image et a. : JurisData n° 2011-023099 ; AJDA 2012, p. 35, chron. M. Guyomar et X. Domino. - V. Tchen, La base de données du passeport biométrique : Dr. adm. 2012, comm. 1. - F. Chaltiel, Le passeport devant le Conseil d'État : LPA 14 déc. 2011, n° 248, p. 10 ;

집·보존하는 것도 마찬가지이다.¹⁵⁾

개인적 특성이 담긴 정보 다시 말해서 민감한 개인정보를 다룰 때는 ① 수집과 처리의 공정성(loyauté), ② 수집 목적의 확정·명백·정당성 (finalités déterminées, explicites et légitimes d'une collecte), ③ 정보처리 실시에서의 비례성(proportionnalité de la mise en oeuvre du traitement), ④ 처리되는 개인정보의 정확성과 완전성(caractère exact et complet des données personnelles traitées), ⑤ 보존기간(durée de conservation)의 준수, ⑥ 사전동의(consentement préalable)를 얻을 것 등이다¹⁶⁾. 이러한 원칙을 준수한 정당하고 적법한 정보처리였는지 여부는 물론 궁극적으로 법원의 판결을 통하기도 하지만 상당 부분 CNIL이 결정한다. 최근의 유명한 결정으로는 근로시간 감독을 위해 생체정보를 이용하는 것은 근로장소에 대한 보안의 경우와는 달라서 인권을 침해하는 부당한 처사라고 본 사례¹⁷⁾가 있다.

절차상으로는 사전절차인 신고(déclaration)나 허가(autoirisation)를 충족해야 할 수도 있다.¹⁸⁾

「정보, 문서 그리고 자유에 관한 1978년 1월 6일자 법률 제78-17호」에 대한 2004년 8월 6일자 개정법률은 사람들의 신원 관리에 필요한 생체정보를 포함한 자동화 처리를 위한 조치를 취하기 위해서는 국가

AJDA 2011, p. 2036, note R. Grand. - CJUE, 17 oct. 2013, aff. C-291/12, Schwarz c/ Stadt Bochum, point 29 : Europe 2013, comm. 512, obs. F. Gazin.

15) CJCE, 16 déc. 2008, aff. C-524/06, Heinz Huber, point 43 : Rec. CJCE 2008, I, p. 9705 ; Europe 2009, comm. 53, obs. F. Kauff-Gazin ; JCP A 2009, 2189, obs. M. Gautier.

16) V. Romain Perray, JurisClasseur Administratif, Fasc. 274-20 : INFORMATIQUE . - Données à caractère personnel . - Conditions de licéité des traitements de données à caractère personnel.

17) CNIL, délib. n° 2012-322, 20 sept. 2012 : Journal Officiel du 12 Octobre 2012 ; JCP E 2012, act. 665.

18) V. Romain Perray, JurisClasseur Administratif, Fasc. 274-30 : INFORMATIQUE . - Données à caractère personnel . - Formalités préalables à la mise en oeuvre d'un traitement de données à caractère personnel.

정보자유위원회(CNIL)의 사전허가(autorisation préalable)를 얻도록 규정하였다. 생체인식기술과 생체정보의 축적에 대한 국가정보자유위원회의 입장은 보안에 관한 문제에서는 우호적인 편이었고, 반면에 학교급식이나 노동현장에서의 사용에는 부정적인 입장이었다.¹⁹⁾

2. 공적 신분의 확인

공공당국으로부터 자신의 신원을 밝힐 것을 요구받은 사람은, 반드시 국민신분증(carte nationale d'identité)에 국한되지는 않고, “모든 수단을 동원하여” 자유롭게 그것을 증명할 수 있다.²⁰⁾ 이 증명방법에 신뢰성을 부여하자는 명분으로 정부는 정보화처리된 이른바 ‘보안국민신분증(carte nationale d'identité sécurisée)’을 창설하여 1995년에 전국적으로 시행하였고²¹⁾, 이어서 ‘보안전자국민신분증(carte d'identité nationale électronique sécurisée)’을 시행하는 내용의 법안을 2003년에 추진하였으나 반발에 부딪혀 보류하였다²²⁾. 안보를 이유로 한 전자여권(passeport électronique)의 시행은 인정되어 시행되었다.²³⁾

3. 민사관계에서의 신분 확인

민사관계에서도 신분 확인은 역시 중요하다. 민사 관계에서의 신분 확인 역시 자유로운 증명의 원칙을 따르고 있는데, 서면을 작성할 경

19) Pierre LECLERCQ, « À propos de la biométrie . - (Quelques réflexions après visite de l'exposition « Biométrie, le corps identité » à la Cité des sciences) », Communication Commerce électronique n° 3, Mars 2006, étude 7.

20) 형사소송법전 제78-2조 제1항.

21) V. D. n° 87-178, 19 mars 1987 portant création d'un système de fabrication et de gestion informatisée des cartes nationales d'identité. - D. n° 87-179, 19 mars 1987 relatif au relevé d'une empreinte digitale lors d'une demande de carte nationale d'identité. - D. n° 99-973, 25 nov. 1999. - D. n° 2007-391, 21 mars 2007.

22) Jacques BUISSON, JurisClasseur Procédure pénale, Fasc. 10 : CONTRÔLES, VÉRIFICATIONS ET RELEVÉS D'IDENTITÉ . - Contrôles et relevés d'identité, n° 55.

23) D. n° 2005-1726, 30 déc. 2005 : Journal Officiel du 31 Décembre 2005.

우 서명(signature)의 진정성을 확인하는 것이 중요하다고 할 수 있다. 「유럽연합 내 전자서명을 위한 1999년 12월 13일자 지침」의 국내법적 전환을 위해 제정된 2000년 3월 13일자 법률 제2000-230호에 의해 서명의 개념을 재정립²⁴⁾하고 전자매체(support électronique)에 의한 증서 작성을 허용²⁵⁾함으로써 전자서명(signature électronique)을 신분확인 수단으로 사용할 수 있는 길을 열었다. 국내시장에서의 전자상거래에 관여하는 정보통신회사들의 법적 측면을 손질한 2000년 6월 8일자 지침 제2000-31호에 의해서도 전자문서 작성과 전자서명이 활성화될 수 있는 제도적 기반이 구축되었다. 전자서명을 위해서는 제3자에 의한 인증이 거치게 하고 이것을 전자인증서비스제공자(prestataire de services de certification électronique)가 담당하도록 하였다. 이것은 제도가 기술발전을 선도한 예로 볼 수 있다.²⁶⁾ 이 부분에서는 특히 보안이 중요한데, 당사자가 아닌 사람이 오가는 전자문서를 볼 수 없도록 암호화(cryptologie)하여 전송하는 기술과 타인이 의사교환 통신망에 침투한 경우 경보를 알려줄 수 있는 시스템을 구축하여야 한다. 이 점에서 생체인식이 기여하고 있으며 앞으로도 기대된다.²⁷⁾

프랑스 최고행정법원인 콩세이테따(Conseil d'État)는 2개의 지문정보만을 수집하도록 되어 있는 유럽연합의 규범과는 달리 내무부장관이 8개의 지문정보를 수집하고 보존하는 것을 허용하는 내용의 「생체정보가 담긴 여권에 관한 2008년 4월 30일자 데크레 제2008-426호」를 위법하다고 판정하였다.²⁸⁾ 헌법재판소(Conseil constitutionnel)는 한술 더 떠

24) C. civ., art. 1316 à 1316-4 et D. n° 2001-272, 30 mars 2001.

25) C. civ., art. 1317, al. 2.

26) Didier GUÉVEL, JurisClasseur Civil Code, Fasc. 40 : CONTRATS ET OBLIGATIONS . - Preuve testimoniale . - Liberté des preuves en matière commerciale, n° 23.

27) Didier GUÉVEL, JurisClasseur Civil Code, Fasc. 40 : CONTRATS ET OBLIGATIONS . - Preuve testimoniale . - Liberté des preuves en matière commerciale, n° 23.

28) CE, ass., 26 oct. 2011, n° 317827, Assoc. pour la promotion de l'image et a. :

서 개인별 신원문서를 국가에서 모아 파일로 만드는 사업을 하는 내용의 테크레를 위헌이라고 결정하였다. 생체정보 등이 담길 수 있는 이러한 자료들의 민감한 성격과 국민 대다수에 관한 취급이라는 규모를 감안할 때 헌법에 위반된다고 판단함에 주저할 필요가 없다는 것이었다.²⁹⁾ 특히 경찰문서로 사용될 경우의 위험성에 대한 우려가 컸고 이것이 위헌판단에 영향을 줄 정도로 문제가 되었던 것으로 보인다.³⁰⁾

4. 생체정보가 담긴 여권

「외국인의 입국 및 체류와 망명권 법전」 L. 611-6조³¹⁾는 Schengen조약(1990년 6월 19일 체결) 가맹국이 아닌 나라의 국민이 프랑스에 머물고자 비자를 신청한 경우에는 「정보, 문서 그리고 자유에 관한 1978년 1월 6일자 법률 제78-17호」가 정한 바에 따라 사진과 함께 지문을 전자적 방식으로 등록할 것을 규정하였다. 이것은 비자 소지인의 신원 확인을 목적으로 ‘비자신청자에게 적용된 생체인식(BIODEV)’

JurisData n° 2011-023099 ; AJDA 2012, p. 35, chron. M. Guyomar et X. Domino. - V. Tchen, La base de données du passeport biométrique : Dr. adm. 2012, comm. 1. - F. Chaltiel, Le passeport devant le Conseil d'État : LPA 14 déc. 2011, n° 248, p. 10 ; AJDA 2011, p. 2036, note R. Grand.

29) Cons. const., 22 mars 2012, déc. n° 2012-652 DC : Rev. Lamy dr. immat. juin 2012, n° 2783, obs. L. Costes ; AJDA 2012, p. 623, note R. Grand. - V. Tchen, L'informatisation des documents d'identité numérisés : Dr. adm. 2012, comm. 48 ; Dr. famille 2012, alerte 29, obs. M. Bruggeman. - F. Mattatia, La loi sur la protection de l'identité est-elle conforme à la Constitution ? : LPA 24 avr. 2012, n° 82, p. 6. - C. Guerrier, La CNI biométrique française : entre préservation de l'identité et protection des libertés individuelles : Rev. Lamy dr. immat. 2012, n° 82, n° 2758.

30) F. Bottini, À quand une question prioritaire de constitutionnalité sur le cadre législatif des fichiers de police ? : JCP A 2011, 2176), sans parler d'une évolution éventuelle de la loi sur ce point (Rapp. info. n° 1548, 24 mars 2009. - S. Lavric, Fichiers de police : publication d'un rapport parlementaire : Rapp. Sénat n° 93, 6 nov. 2009. - O. Proust, État des lieux sur la proposition de loi du Sénat visant à modifier la loi "Informatique et libertés" : Rev. Lamy dr. immat. 2009, n° 55, n° 1823.

31) D. n° 2004-1266, 25 nov. 2004 : Journal Officiel du 26 Novembre 2004.

이다.³²⁾ 이에 대하여 국가정보자유위원회는 국경통제의 목적과 생체 정보를 저장하고 보존하는 것 사이에는 적절한 관계가 없고 정당하지 않다는 의견³³⁾을 낸 바 있다. 2008년 3월 6일자 데크레 제2008-223호에 의해 이 법전의 R. 211-1조가 개정되어 비자를 소지한 외국인이 프랑스에 입국할 때 비자에 등록된 지문정보와의 일치 여부를 확인하기 위해 지문검사를 할 수 있도록 하는 근거규정을 마련하였다. 제출된 생체정보는 입력된 후 자동적으로 처리된다.³⁴⁾

32) Xavier VANDENDRIESSCHE, JurisClasseur Civil Code, Fasc. 11 : ÉTRANGERS .
- Entrée en France n° 42

33) CNIL, délib. n° 2004-075, 5 oct. 2004 : Journal Officiel du 4 Décembre 2004.

34) Annexe 6.3 mentionnée à l'article R. 611-9 du Code de l'entrée et du séjour des étrangers et du droit d'asile)-II-c.

미국의 생체정보 관련 법제 동향

이 상 경
(서울시립대 법전원 교수)

I. 서

생체인식이란 개인을 특정하는데 사용될 수 있는 얼굴의 특징, 망막이나 홍채의 패턴, 지문 등 신체적 특징들의 측정을 말한다. 이러한 특정화에 사용될 수 있는 개인의 다양한 신체적 정보를 생체인식정보라 할 수 있다. 생체인식정보의 수집 및 활용을 증진하고 장려하는 방안에 대한 연구도 필요하지만, 생체인식정보의 수집·활용기술의 발전으로 인하여 나타날 수 있는 문제점을 방지하거나 해결하기 위하여 미국의 생체정보와 관련된 사례 및 법제를 연구, 검토할 필요가 있다.

II. 미국 연방의 법제 동향

1. 미국 연방 생체인식정보 활용 프로그램

- (1) 연방상무부(통상교역부: Department of Commerce)
국가표준기술원(National Institute of Standards and Technology)

국가표준기술원에서는 지문의 일치여부와 호환(fingerprint matching and interchange), 형사사법정보체계(criminal justice information systems), 얼굴인식 및 다양한 형태의 생체인식정보(face recognition and multi-modal biometrics)에 대한 측정, 평가 및 표준(measurement, evaluation and standards)에 대한 연구를 수행한다. 국가표준기술원은 1960년대 연방수사국의 법집행과 과학수사기술을 지원하기 위한 지문정보기술에 대한 연구와 더불어 지난 50년간 생체인식정보분야에서 연구를 수행해 왔다. 국토안

보의 요청이 증대되자 생체인식은 개인의 특정을 위한 핵심기술로 더욱 중요성이 커졌다. 국가표준원은 그 임무와 추적자료(track record) 덕분에 양질의 생체인식정보의 수집을 증대시키는 광범위한 정부차원의 노력을 지원하게 되었고, 이로써 수집된 자료가 다른 기관에 의해 적절히 공유되도록 하며, 생체인식시스템의 정확성과 상호활용성이 확실하게 증대될 수 있도록 하였다. 국가표준기술원의 생체인식활용은 첫째, 지문, 얼굴, 홍채, 음성, DNA 및 복합형태생체정보 등 다양한 형태의 생체인식정보를 연구한다. 둘째, 국내적 그리고 국제적인 수준에서의 표준기술의 개발에 이바지하며, 셋째, 혁신을 위하여 생체인식관련 기술을 시험하고 측정한다.

(2) 국방부 국방과학수사 및 생체인식국(Department of Defense Defense Forensics and Biometrics Agency)의 생체인식관리워크샵(Biometric Quality Workshop)

DFBA는 동일성판단과정을 지원함으로써 국방부의 생체인식활동과 과학수사에 공조하고 강화하는데 기여한다.

(3) 국토안보부(Department of Homeland Security)

1) 진정신분증명(REAL ID.)

REAL ID는 테러를 막고, 사기를 감소시키며, 연방정부가 발행한 신분증명서류의 정확도와 신뢰성을 제고하기 위한 전국적인 차원의 노력이다. 2007년 3월 1일, 국토안보부는 진정신분증명법 제정을 위한 60일간의 코멘트 기간을 공지[a Notice of Proposed Rulemaking (NPRM)]하였다. NPRM은 진정신분증명에 적응하는 운전면허나 ID카드에 요구되는 특성으로서의 생체인식정보를 포함하지 않고 있었으나, 장래 추가적인 보안의 요소로, 또 재발급기간동안 개인을 확인하기 위한 요소로, 각 주가 이를 요청할 수 있는 가능성에 대한 코멘트를 유도하였다.

2) 생체인식관리사무국(Office of Biometric Identity Management (OBIM).

연방의회의 권고로 미 국방부산하에 바이오매트릭스기술을 도입할 목적으로 생체인식관리사무국의 전신으로 2000년에 설립된 것이 바이오정보관리사무국(Biometrics Management Office: BMO)이다. 2003년 9월에 거행된 바이오매트릭스컨소시엄 회의에서 「바이오매트릭스 프라이버시에 관한 국방부 가이드스」를 공표하였다. 이는 미국 국방부내에서의 바이오매트릭스와 관련된 프라이버시 보호를 위한 프로그램이나 프레임워크의 제공을 목적으로 하고 있는데, 여기에는 「[1] 프라이버시권의 보호에 관한 가이드스, [2] 바이오매트릭스 정보의 수집권한에 관한 가이드스, [3] 바이오매트릭스정보 보호를 위한 국방부의 책임」이란 세 가지 항목에 관한 기준을 제시하는 내용으로 구성되어 있다.¹⁾ OBIM는 2013년 3월에 the United States Visitor and Immigration Status Indicator Technology (US-VISIT)²⁾를 대체하고 현대화하기 위하여 창립되었다.

1) 국방부 Guidance에 관해서는 Department of Defense Biometrics Management Office Privacy Approach

<[http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20PowerPoint%20-%205_BMO_M_Wendling.ppt%20\[Read- Only\]%20\[Re.pdf](http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20PowerPoint%20-%205_BMO_M_Wendling.ppt%20[Read-Only]%20[Re.pdf)> 참조.

2) 미국의 출입국관리시스템을 보면 미국 출입국관리의 핵심인 US-VISIT 프로그램은 입국 외국인의 생체정보를 채취하여 watch list 및 범법자 정보 등과 비교를 수행한다. US-VISIT은 1996년 IIRIRA(불법이민개혁법)에서 요청된 자동화 출입국관리시스템으로부터 시작되었으며, 2004년 ‘정보개혁 및 테러방지법’에서 US-VISIT을 자동화된 생체출입국데이터시스템으로 정의하였다. 2004년 입국 외국인의 2지 (양손 검지) 지문과 사진 수집을 시작하였으며, 2007년부터 정확도 향상과 호환성 지원을 위해 10지 지문과 사진 수집 방식으로 변경되었다. 미국 입국 외국인의 철저한 신원확인을 위해 비자 신청자에 대한 생체정보 수집 및 검증과 입국 시 생체정보 신원확인 과정을 거치고 있으며, 국토안보부 산하 이민관련기관들에서는 수집된 생체정보를 이용하여 위조문서를 사용하거나 신원 도용한 방문자를 막고, 수천의 범죄자와 출입국 사범들의 입국금지 판정에 활용하고 있다. <http://consulting.skcc.com/39> 참조 (마지막 방문 2016. 6. 15).

3) 운송업무종사자신분증명

(The Transportation Worker Identification Credential: TWIC)

TWIC은 모든 종류의 운송수단에 활용될 수 있는 시스템확장적인 공용자격증명체계이다. TWIC는 국가운송시스템의 보안영역에 대해 단독으로(unesorted) 물리적(신체적) 접근 및/혹은 컴퓨터에 의해 접근하는 모든 승무원들을 위하여 활용될 수 있다. TWIC는 운송체계가 위협에 노출되기 쉬운 속성을 고려하여 고안된 것이다. TWIC는 Aviation and Transportation Security Act (ATSA) and the Maritime Transportation Security Act (MTSA)의 입법규정들에 따라 만들어 졌다.

4) 등록여행자(Registered Traveler)

운송안전국[The Transportation Security Administration (TSA)]은 현재 항공안전의 강화와 세관(customer service)의 증대를 위한 목적으로 민간영역과 더불어 등록여행자프로그램(Registered Traveler Program)을 개발 중이다. 등록여행자프로그램은 운송안전국의 감시와 더불어 사적영역에서 제공되는 자율적인 시장 주도 프로그램이 될 것이다. 기업들은 생체정보(지문과 홍채)와 바이오그래픽 정보를 활용하는 등록여행자프로그램의 참여자가 될 것이다.

5) 연결(NEXUS)

NEXUS는 다양한 형태로 미국과 캐나다를 출입하는 여행객들을 위한 프로그램이다.³⁾

3) NEXUS Air enrollees use automated kiosks located in the U.S. Preclearance area and Canadian Inspection Services area at Vancouver International Airport for validation. At these locations, travelers present their membership card, submit their iris for biometric verification, and make a declaration. Upon successful completion of the above, the traveler is directed to the exit.

(4) 법무부(Department of Justice)

1) 연방수사국(FBI) 생체인식표준(Biometric Standards)

연방수사국은 생체인식표준으로 전자지문전송명세서[Electronic Fingerprint Transmission Specification (EFTS)) Version 8.0을 사용한다.⁴⁾

2) 통합자동지문인식체계

(The Integrated Automated Fingerprint Identification System: IAFIS)

IAFIS는 연방수사국의 형사사법정보서비스부서[Criminal Justice Information Services (CJIS) Division].에 의해 운용되는 전국적 지문 및 범죄 기록 시스템이다. IAFIS는 365일 24시간 자동지문검색능력, 잠재적 검색 능력, 전자적 이미지 저장 및 지문의 전자적 교환과 응답을 위한 서비스를 제공한다.

3) 연방수사국의 차세대 신원확인 시스템

(The FBI's Next Generation Identification System : NGI)

NGI는 현존하는 IAFS 환경 하에서 검색, 평가, 구현을 위한 진보된 기술을 통하여 생체인식신원확인과 범죄기록정보서비스를 확장하고 개선하여 테러범죄자와 범죄행위를 감소시키기 위해 수년간 이루어진 노력의 결과물이다.

4) 국가사법연구원(The National Institute of Justice : NIJ)

NIJ는 능동적 생체인식프로그램을 보유하며, 종종 연방기구들과 생체인식연구개발테스트와 평가[biometric Research Development Test and Evaluation (RDT&E)]를 증대시키기 위한 노력을 공조, 협업함으로써, 연방과 지방 차원의 범죄와 형사사법의 변화에 적응하는 임무에 대처한다.

4) About other FBI biometric-related specifications, please visit the official FBI Biometric Standards website.

5) 생체인식특성화센터[The Biometric Center of Excellence (BCOE)]

BCOE는 웨스트 버지니아의 Clarksburg에 본부를 두고 있는 기구로 연방수사국의 생체인식과 신원확인 운용의 핵심조직이다. 연방수사국의 과학기술부(The FBI's Science and Technology Branch)는 프라이버시법, 정책, 그리고 절차에 부합하는 것을 보장하면서도 최첨단의 생체인식기술로 범죄와 테러리즘과 싸울 수 있는 능력을 강화하기 위하여 창설되었다. BCOE는 생체인식협업(협동)과 전문가들의 원스톱상점이나 마찬가지로, 즉, 과학자, 전문기술자, 그리고 생체인식 전문가들이 BCOE의 임무를 수행해 나가고 있으며, 이는 연방수사국과 사법집행부서 및 국가안보조직들의 범주 내에서 협업을 장려하고, 정보공유를 증대시키며, 최적의 생체인식과 신원확인의 운용솔루션을 채용하는 기술을 진보시키기 위한 것이다. (scientists, technicians, and biometrics experts are advancing the BCOE's mission to foster collaboration, improve information sharing, and advance the adoption of optimal biometric and identity management solutions within the FBI and across the law enforcement and national security communities)

(5) 국무부(Department of State)

1) 미국 전자여권(US Electronic Passport)

U.S. Electronic Passport는 일반 여권과 동일하나 뒷면 커버에 작은 무접촉성의 통합서킷(컴퓨터칩)이 부가된 것이다. 이 칩은 여권의 사진부착면에 시각적으로 인식될 수 있는 사항과 동일한 데이터를 저장하고 있으며, 디지털 사진을 내장하고 있다. 디지털 사진의 내장은 국경에서 얼굴(안면)인식기술을 통하여 생체인식 비교를 가능하게 한다. U.S. "e-passport"는 또한 새로운 모습을 갖고 있고, 추가적으로 위조방지과 보안을 위한 특성을 체화시킨 것이다.

2) 보안네트워크접근(Secure Network Access)

보안네트워크진정성증명(Secure network authentication)은 현재 스마트카드와 생체인식을 활용하여 가능하게 되었다. 사용자들은 단순히 그들의 스마트카드를 생체인식 판독기에 삽입하고 그들의 손가락을 판독기 표면에 올려놓음으로써 생체인식진정증명이 가능하다. 이러한 솔루션은 사용자들을 위한 생생하고도 카드상의 매칭 기술을 시연하는바, 이를 통하여 모든 절차가 카드 판독기를 통하여 이루어지게 된다. 카드 판독기를 통한 절차를 통하여, 사용자진정증명에 소요되는 시간을 실질적으로 감소시키며, 이는 사용자의 정보가 워크스테이션을 통하여 인증될 필요가 없어지기 때문이다. 이러한 기술의 최대 이익은 활용이 쉽다는 것이며, 비밀번호 공유에 따른 위조의 위험을 감소시키고, 패스워드 리셀 절차가 제거된다는데 있다. 제거에 따른 위조위험을 감소시키는데 있다.

(6) 신원확인기술연구센터

(The Center for Identification Technology Research: CITeR.)

2001년부터 CITeR는 국가과학재단 산업 및 대학 협업 연구센터였다. 센터의 주된 목적은 기초, 자동화된 생체인식 시스템의 활용과 평가를 위한 새로운 기술과 관련된 연구개발행위에 대한 최첨단의 연구를 수행하는데 있다. 또한 멤버십에 의하여 사적 영역 및 공적 영역에서 새로운 생체 기술을 적시에 효율적으로 이전하는데 목적이 있으며, 생체인식 연구에서 과학자와 기술자들의 학제적인 훈련을 장려하는데 있다.

2. 관련 대통령 명령(Presidential Directives)

아래의 Presidential Directives는 직접 또는 간접적으로 생체인식 요서를 포함하고 있다.

(1) NSPD-59/HSPD-24

National Security Presidential Directive (NSPD)-59 / Homeland Security Presidential Directive (HSPD) - 24, 국가안보의 증대를 위한 신원확인 및 선별차단 생체인식 명령은 2008년 6월 5일 부시 대통령에 의해 서명되었다 (“Biometrics for Identification and Screening to Enhance National Security,” was signed by President Bush on June 5, 2008). 이 대통령 명령은 연방정부와 연방기구들이 미국 연방법 아래에서 프라이버시와 법적인 권리들을 존중하면서도, 적법하고 적절한 방법으로 개인의 생체인식과 관련된 바이오그래픽 및 전후 관련된 정보의 공유, 분석, 활용, 저장 및 수집에 있어 법에 상응하는 방법과 절차를 활용하도록 보장하는 법적인 틀을 제공한다(This directive establishes a framework to ensure Federal departments and agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting privacy and other legal rights under United States law). 이 대통령 명령은 현존하는 조율노력과 협조 위에서 정부전체를 통관하여 높은 수준의 계획들을 보장하는데 있다(This directive builds upon existing coordination efforts and helps to ensure that high-level plans are implemented throughout government). 이 명령은 주정부, 지방, 부락(부족) 정부에 대하여 의무를 부과하지 않는다(This directive does not impose requirements on State, local, or tribal authorities, or on the private sector). 이 명령은 또한 정보의 수집, 보유 또는 보급을 위한, 혹은 신원확인 또는 선별행위를 위한 새로운 연방정부의 권한을 부여하지도 않는다(It also does not provide new Federal authority for collection, retention, or dissemination of information, or for identification

and screening activities).⁵⁾

5) **National Security Presidential Directive and Homeland Security Presidential Directive
NSPD-59 / HSPD-24** June 5, 2008

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD – 59

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD – 24

SUBJECT: Biometrics for Identification and Screening to Enhance National Security Purpose

This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.

Scope

- (1) The executive branch has developed an integrated screening capability to protect the Nation against "known and suspected terrorists" (KSTs). The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and other persons who may pose a threat to national security.
- (2) Existing law determines under what circumstances an individual's biometric and biographic information can be collected. This directive requires agencies to use, in a more coordinated and efficient manner, all biometric information associated with persons who may pose a threat to national security, consistent with applicable law, including those laws relating to privacy and confidentiality of personal data.
- (3) This directive provides a Federal framework for applying existing and emerging biometric technologies to the collection, storage, use, analysis, and sharing of data in identification and screening processes employed by agencies to enhance national security, consistent with applicable law, including information privacy and other legal rights under United States law.
- (4) The executive branch recognizes the need for a layered approach to identification and screening of individuals, as no single mechanism is sufficient. For example, while existing name-based screening procedures are beneficial, application of biometric technologies, where appropriate, improve the executive branch's ability to identify and screen for persons who may pose a national security threat. To be most effective, national security identification and screening systems will require timely access to the most accurate and most complete biometric, biographic, and related data that are, or can be, made available throughout the executive branch.
- (5) This directive does not impose requirements on State, local, or tribal authorities or on the private sector. It does not provide new authority to agencies for collection,

retention, or dissemination of information or for identification and screening activities.

Definitions

(6) In this directive:

- (a) “Biometrics” refers to the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition; and
- (b) “Interoperability” refers to the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Background

- (7) The ability to positively identify those individuals who may do harm to Americans and the Nation is crucial to protecting the Nation. Since September 11, 2001, agencies have made considerable progress in securing the Nation through the integration, maintenance, and sharing of information used to identify persons who may pose a threat to national security.
- (8) Many agencies already collect biographic and biometric information in their identification and screening processes. With improvements in biometric technologies, and in light of its demonstrated value as a tool to protect national security, it is important to ensure agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information.
- (9) Building upon existing investments in fingerprint recognition and other biometric modalities, agencies are currently strengthening their biometric collection, storage, and matching capabilities as technologies advance and offer new opportunities to meet evolving threats to further enhance national security.
- (10) This directive is designed to (a) help ensure a common recognition of the value of using biometrics in identification and screening programs and (b) help achieve objectives described in the following:

Executive Order 12881 (Establishment of the National Science and Technology Council); Homeland Security Presidential Directive-6 (HSPD-6) (Integration and Use of Screening Information to Protect Against Terrorism); Executive Order 13354 (National Counterterrorism Center); Homeland Security Presidential Directive-11 (HSPD-11) (Comprehensive Terrorist Related Screening Procedures); Executive Order 13388 (Further Strengthening the Sharing of Terrorism Information to Protect Americans); National Security Presidential Directive-46/Homeland Security Presidential Directive-15 (NSPD-46/HSPD-15) (U.S. Policy and Strategy in the War on Terror); 2005 Information Sharing Guidelines; 2006 National Strategy for Combating Terrorism; 2006 National Strategy to Combat Terrorist Travel; 2007 National Strategy for Homeland

Security; 2007 National Strategy for Information Sharing; and 2008 United States Intelligence Community Information Sharing Strategy.

Policy

- (11) Through integrated processes and interoperable systems, agencies shall, to the fullest extent permitted by law, make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security.
- (12) All agencies shall execute this directive in a lawful and appropriate manner, respecting the information privacy and other legal rights of individuals under United States law, maintaining data integrity and security, and protecting intelligence sources, methods, activities, and sensitive law enforcement information.

Policy Coordination

- (13) The Assistant to the President for Homeland Security and Counterterrorism, in coordination with the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy, shall be responsible for interagency policy coordination on all aspects of this directive.

Roles and Responsibilities

- (14) Agencies shall undertake the roles and responsibilities herein to the fullest extent permitted by law, consistent with the policy of this directive, including appropriate safeguards for information privacy and other legal rights, and in consultation with State, local, and tribal authorities, where appropriate.
- (15) The Attorney General shall:
 - (a) Provide legal policy guidance, in coordination with the Secretaries of State, Defense, and Homeland Security and the Director of National Intelligence (DNI), regarding the lawful collection, use, and sharing of biometric and associated biographic and contextual information to enhance national security; and
 - (b) In coordination with the DNI, ensure that policies and procedures for the consolidated terrorist watchlist maximize the use of all biometric identifiers.
- (16) Each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall:
 - (a) Develop and implement mutually compatible guidelines for each respective agency for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information, to the fullest extent practicable, lawful, and necessary to protect national security;
 - (b) Maintain and enhance interoperability

among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols, and interfaces; (c) Ensure compliance with laws, policies, and procedures respecting information privacy, other legal rights, and information security; (d) Establish objectives, priorities, and guidance to ensure timely and effective tasking, collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information among authorized agencies; (e) Program for and budget sufficient resources to support the development, operation, maintenance, and upgrade of biometric capabilities consistent with this directive and with such instructions as the Director of the Office of Management and Budget may provide; and (f) Ensure that biometric and associated biographic and contextual information on KSTs is provided to the National Counterterrorism Center and, as appropriate, to the Terrorist Screening Center.

- (17) The Secretary of State, in coordination with the Secretaries of Defense and Homeland Security, the Attorney General, and the DNI, shall coordinate the sharing of biometric and associated biographic and contextual information with foreign partners in accordance with applicable law, including international obligations undertaken by the United States.
- (18) The Director of the Office of Science and Technology Policy, through the National Science and Technology Council (NSTC), shall coordinate executive branch biometric science and technology policy, including biometric standards and necessary research, development, and conformance testing programs.

Recommended executive branch biometric standards are contained in the Registry of United States Government

Recommended Biometric Standards and shall be updated via the NSTC Subcommittee on Biometrics and Identity Management.

Implementation

- (19) Within 90 days of the date of this directive, the Attorney General, in coordination with the Secretaries of State, Defense, and Homeland Security, the DNI, and the Director of the Office of Science and Technology Policy, shall, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, submit for the President's approval an action plan to implement this directive. The action plan shall do the following: (a) Recommend actions and associated timelines for enhancing the existing terrorist-oriented identification and screening processes by expanding the use of biometrics; (b) Consistent with applicable law, (i) recommend categories of individuals in addition to KSTs who may pose a threat to national security, and (ii) set forth cost-effective actions and associated timelines for expanding the collection and use of biometrics to identify and screen for such individuals; and (c) Identify

(2) HSPD-12

Homeland Security Presidential Directive (HSPD)-12 specifies a policy for a common identification standard for federal employees and contractors. The standard calls for interoperable fingerprint minutia to be used for interagency biometric verification; agencies may also use other biometrics for own-employee verification.⁶⁾

business processes, technological capabilities, legal authorities, and research and development efforts needed to implement this directive.

- (20) Within 1 year of the date of this directive, the Attorney General, in coordination with the Secretaries of State, Defense, and Homeland Security, the DNI, and the heads of other appropriate agencies, shall submit to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, a report on the implementation of this directive and the associated action plan, proposing any necessary additional steps for carrying out the policy of this directive. Agencies shall provide support for, and promptly respond to, requests made by the Attorney General in furtherance of this report. The Attorney General will thereafter report to the President on the implementation of this directive as the Attorney General deems necessary or when directed by the President.

General Provisions

- (21) This directive:
- (a) shall be implemented consistent with applicable law, including international obligations undertaken by the United States, and the authorities of agencies, or heads of such agencies, vested by law;
 - (b) shall not be construed to alter, amend, or revoke any other NSPD or HSPD in effect on the effective date of this directive;
 - (c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable by law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

6) Homeland Security Presidential Directive/Hspd-12 August 27, 2004

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

- (1) Wide variations in the quality and security of forms of identification used to gain

access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

- (2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the “Standard”) not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.
- (3) “Secure and reliable forms of identification” for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).
- (4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.
- (5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not

(3) HSPD 11 : Comprehensive Terrorist-Related Screening Procedures⁷⁾

covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

- (6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.
- (7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.
- (8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

7) Homeland Security Presidential Directive/Hspd-11 August 27, 2004

Subject: Comprehensive Terrorist-Related Screening Procedures

- (1) In order more effectively to detect and interdict individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (“suspected terrorists”) and terrorist activities, it is the policy of the United States to: (a) enhance terrorist-related screening (as defined below) through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security, and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law, and builds upon existing risk assessment capabilities while facilitating the efficient movement of people, cargo, conveyances, and other potentially affected activities in commerce; and (b) implement a coordinated and comprehensive approach to terrorist-related screening -- in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure -- that supports homeland security, at home and abroad.
- (2) This directive builds upon HSPD-6, “Integration and Use of Screening Information to Protect Against Terrorism.” The Terrorist Screening Center (TSC), which was established and is administered by the Attorney General pursuant to HSPD-6, enables Government officials to check individuals against a consolidated Terrorist

Screening Center Database. Other screening activities underway within the Terrorist Threat Integration Center (TTIC) and the Department of Homeland Security further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism.

- (3) In this directive, the term “terrorist-related screening” means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.
- (4) Not later than 75 days after the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretaries of State, Defense, Transportation, Energy, Health and Human Services, Commerce, and Agriculture, the Directors of Central Intelligence and the Office of Management and Budget, and the heads of other appropriate Federal departments and agencies, shall submit to me, through the Assistant to the President for Homeland Security, a report setting forth plans and progress in the implementation of this directive, including as further described in sections 5 and 6 of this directive.
- (5) The report shall outline a strategy to enhance the effectiveness of terrorist-related screening activities, in <http://www.fas.org/irp/offdocs/nspd/hspd-11.html> (1 of 3)6/16/2008 12:00:05 PM Homeland Security Presidential Directive / HSPD-11: Comprehensive Terrorist-Related Screening Procedures accordance with the policy set forth in section 1 of this directive, by developing comprehensive, coordinated, systematic terrorist-related screening procedures and capabilities that also take into account the need to:
 - (a) maintain no less than current levels of security created by existing screening and protective measures;
 - (b) encourage innovations that exceed established standards;
 - (c) ensure sufficient flexibility to respond rapidly to changing threats and priorities;
 - (d) permit flexibility to incorporate advancements into screening applications and technology rapidly;
 - (e) incorporate security features, including unpredictability, that resist circumvention to the greatest extent possible;
 - (f) build upon existing systems and best practices and, where appropriate, integrate, consolidate, or eliminate duplicative systems used for terrorist-related screening;
 - (g) facilitate legitimate trade and travel, both domestically and internationally;
 - (h) limit delays caused by screening procedures that adversely impact foreign relations, or economic, commercial, or scientific interests of the United States; and
 - (i) enhance information flow between various screening programs.
- (6) The report shall also include the following:
 - (a) the purposes for which individuals will undergo terrorist-related screening;
 - (b) a description of the screening opportunities to which terrorist-related screening will be applied;

-
- (c) the information individuals must present, including, as appropriate, the type of biometric identifier or other form of identification or identifying information to be presented, at particular screening opportunities;
 - (d) mechanisms to protect data, including during transfer of information;
 - (e) mechanisms to address data inaccuracies, including names inaccurately contained in the terrorist screening data consolidated pursuant to HSPD-6;
 - (f) the procedures and frequency for screening people, cargo, and conveyances;
 - (g) protocols to support consistent risk assessment and inspection procedures;
 - (h) the skills and training required for the screeners at screening opportunities;
 - (i) the hierarchy of consequences that should occur if a risk indicator is generated as a result of a screening opportunity;
 - (j) mechanisms for sharing information among screeners and all relevant Government agencies, including results of screening and new information acquired regarding suspected terrorists between screening opportunities;
 - (k) recommended research and development on technologies designed to enhance screening effectiveness and further protect privacy interests; and <http://www.fas.org/irp/offdocs/nspd/hspd-11.html> (2 of 3)6/16/2008 12:00:05 PM Homeland Security Presidential Directive / HSPD-11: Comprehensive Terrorist-Related Screening Procedures (l) a plan for incorporating known traveler programs into the screening procedures, where appropriate.
- (7) Not later than 90 days after the date of this directive, the Secretary of Homeland Security, in coordination with the heads of the Federal departments and agencies listed in section 4 of this directive, shall also provide to me, through the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget, a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan shall describe the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement the policy set forth in section 1 of this directive. The Secretary of Homeland Security shall further provide a report on the status of the implementation of the plan to me through the Assistant to the President for Homeland Security 6 months after the date of this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.
- (8) In order to ensure comprehensive and coordinated terrorist-related screening procedures, the implementation of this directive shall be consistent with Government-wide efforts to improve information sharing. Additionally, the reports and plan required under sections 4 and 7 of this directive shall inform development of Government-wide information sharing improvements.
- (9) This directive does not alter existing authorities or responsibilities of department and agency heads including to carry out operational activities or provide or receive

(4) HSPD 6 : Integration and Use of Screen Information⁸⁾

information. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees, or agents, or any other person.

8) **Homeland Security Presidential Directive / HSPD-6 September 16, 2003**

Subject: Integration and Use of Screening Information

To protect against terrorism it is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes. This directive shall be implemented in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans. To further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism, and to the full extent permitted by law and consistent with the policy set forth above:

- (1) The Attorney General shall establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes.
- (2) The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence in the TTIC's custody, possession, or control that the organization requires to perform its functions.
- (3) The heads of executive departments and agencies shall conduct screening using such information at all appropriate opportunities, and shall report to the Attorney General not later than 90 days from the date of this directive, as to the opportunities at which such screening shall and shall not be conducted.
- (4) The Secretary of Homeland Security shall develop guidelines to govern the use of such information to support State, local, territorial, and tribal screening processes, and private sector screening processes that have a substantial bearing on homeland security.

3. 관련 연방 법제⁹⁾

미국의 공공부문의 경우 1970년대 디지털 정보처리의 확산은 공공과 민간부문 모두에 걸쳐 정보프라이버시 침해에 대한 우려를 야기했다. 개인정보보호를 위하여 1974년 연방법인 프라이버시법(Privacy Act of 1974)이 제정되어 있으나, 민간부문의 경우 포괄적인 법률이 존재하지 않아 기본적으로 자율규제(self-regulation)가 원칙이다. 연방정부는 1974년 공공부문에서 프라이버시법(Privacy Act)을 제정하여 미국 연방 공공기관에 대하여 디지털 기록에 대하여 기록의 안전 및 비밀을 확보하고 정보의 안전 또는 완전성을 보장하기 위해 적절한 행정적, 기술적, 물리적 안전장치를 마련할 것을 규정하였다. 동 법은 후에 ‘컴퓨터 매칭과 개인정보보호에 관한 법률’(Computer Matching and Privacy Protection Act)과 합쳐지면서 개정된다. ‘컴퓨터 매칭과 개인정

(5) The Secretary of State shall develop a proposal for my approval for enhancing cooperation with certain foreign <http://www.fas.org/irp/offdocs/nspd/hspd-6.html> (1 of 2)6/16/2008 11:59:01 AM Homeland Security Presidential Directive / HSPD-6 governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments. This directive does not alter existing authorities or responsibilities of department and agency heads to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person. The Attorney General, in consultation with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence, shall report to me through the Assistant to the President for Homeland Security not later than October 31, 2003, on progress made to implement this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate

9) 미국의 개인정보법제와 생체정보보호법제에 관한 자세한 논의는, 김일환, 생체정보보호법제 정비방안에 관한 고찰, 토지공법연구 제33집 (2006년), 361면 이하; 김일환, 미국의 생체정보보호법제에 관한 연구, 인터넷법률 통권 제31호(2005년), 101면 이하 참조.

보 보호에 관한 법률’은 1988년 미 의회가 통과시킨 법이다. 1977년 미 연방정부는 정부공무원들의 개인정보를 모두 전자화하기 시작하였는데, 데이터베이스가 원래 수집 목적 외로 활용되었다. 그래서 공공기관이 준수해야하는 절차적인 요구사항을 규정한 것이다. 개정된 프라이버시법에서는 공공기관이 개인 정보를 담고 있는 데이터베이스의 존재를 공시하도록 하였다. 그리고 개인으로 하여금 자신의 기록을 접근하고 그 내용을 정정할 수 있는 기회를 제공하도록 하였다. 그리고 공공기관에는 ‘개인정보의 정확성, 적절성, 시의성 및 완전성을 유지할 의무를 부과하였다. 동 법률은 연방정부에 대한 개인정보보호를 규정하고 있어 다른 공공기관에는 적용되지 않아 공공부문에 대한 완전한 일반법으로 보기는 어렵다(5 U.S.C. §552(e)). 동 법은 개인정보의 수집기관이 필요한 한도에서만 정보를 수집 보유하도록 하고 가능한 본인으로부터 수집할 것을 규정하고 있다. 서면요청이나 사전 서명동의에 의하지 않고는 개인정보를 공개 할 수 없도록 하고, 다만 통계목적이나, 연방정부의 목적범위내의 통상적인 사용, 보관 목적, 법집행목적, 의회조사목적 기타 행정목적인 경우에는 예외로 하고 있다. 또한 제3자에 대한 제공은 원칙적으로 법률상 근거에 의해서만 허용되며, 이 경우 그 제공사실을 당사자에게 고지하는데 상당한 노력을 하도록 하고 있다(5 U.S.C. §552a(e)(8)).

정보자유법(Freedom of Information Act)에는 정부의 공공문서에 기록된 정보들을 공개하도록 강제하면서도 프라이버시의 보호를 위한 면제조항을 두고 있다. 즉 “공개하면 개인의 프라이버시에 대한 명백하게 부당한 침해가 되는 인사 및 의료에 관하 파일 기타 이에 유사한 파일”(5 U. S. C. §552(b)(6)), “법집행목적을 위하여 수집된 기록 또는 정보”로서 그의 제공이 개인의 프라이버시에 대한 부당한 침해가 될 것이 합리적으로 예측될 수 있는 경우를 말한다(5 U.S.C. §552(b)(7)(C)). 법원은 정보자유법의 면제조항을 근거로 국가가 보관하고 있는 정보의

공개할 수 있는가에 대한 이익형량의 기준을 ‘주된 목적(central purpose)’의 법리로서 제시하였다. ‘주된 목적’의 법리는 사생활 침해와 정보공개 분쟁에 관계된 판결들에 대한 유력한 분쟁해결의 판단기준으로 채택되었다. 처음으로 제시된 판결은 ‘U. S. Dept. of Justice v. Reporters Committee for Freedom of the Press’ 판결이다. 이 사건은 CBS 방송국과 기자협회가 법무부를 상대로 조직폭력배 4명에 관한 형사 기록을 요구한 데서 비롯되었다. 쟁점은 연방수사국의 컴퓨터에 있는 전과기록을 정보자유법의 면제조항 제7항(c)를 근거로 공개할 수 있는가였다. 즉 민감정보의 공개가 프라이버시를 부당하게 침해할 것으로 합리적으로 예상되는가가 핵심적인 관점이었다. 주요판단의 요지는 컴퓨터에 집적되어 있는 정보는 전과 기록뿐만 아니라 생년월일, 신체적 특징과 같은 사적인 정보를 포함하고 있으므로 실질적인 프라이버시 침해가 발생했다는 것이다. 그래서 당해 기록대장의 제3자 공개는 범주적으로 프라이버시의 부당한 침해에 속한다는 것으로 판결하였다. 이에 반하여 소수의견으로서 해당 행정기관의 행정서비스 결과로 얻어진 정보가 아니라 행정기관이 보유하고 있는 개인정보이기 때문에 사생활 보호의 이익이 사실 상 가장 큰 반면 일반대중의 정보 공개 이익은 가장 약하다는 의견도 있었다. 그래서 사생활 침해는 아니라는 의견이었다. 이 판결은 어느 정도의 범위 내에서 공개할 것인지 그 정도를 고려했다는 점에서는 주목을 받았다.

2004년 미국 연방제9순회항소법원은 2000년 DNA분석보충기록제거법(DNA Analysis Backlog Elimination Act of 2000)이 집행유예(parole)·보호관찰(probation) 혹은 ‘감시조건부 석방’(supervised release)된 연방범죄자들로부터 강제적으로 DNA정보를 추출하여 혈액샘플로 제공하게 한 것은 영장 없는 압수수색을 금지하는 수정헌법 제4조에 위반한 것이 아니라고 판시하였다.¹⁰⁾ 이 판결은 결국 현행 DNA데이터베

10) U.S. v. Kincade, 379 F.3d 813 (Cir. 9th, 2004).

이스와 같이 홍채(iris)·얼굴인식(face recognition) 정보 등의 축적을 위해 유죄판결을 받은 범죄자들에게 생체식별정보를 제출하도록 강제하게 된다. 현재 미국 50개의 주에서 유죄판결을 받은 자들만 DNA 샘플을 제출하도록 요구하고 있고, 집행기관이 DNA프로필을 유지·관리할 수 있도록 규정하고 있으나, 실제로는 아직 유죄판결을 받지 않은 체포된 범죄자들의 DNA프로필도 DNA데이터은행에 축적되고 있다. DNA분석보충기록제거법과 연방법원의 판결은 결과적으로 DNA 샘플 이외의 홍채(iris) 및 얼굴인식 정보 등 생체식별정보를 수집할 수 있는 수단을 제공한다. 사실 DNA샘플을 수집하기 위해 혈액샘플 등을 강제로 채취하는 것과 비교하면, 홍채(iris)나 지문(fingerprint)·화상(image) 정보를 단순히 스캔하는 것은 침해의 정도가 낮으므로 생체식별정보의 수집은 수정헌법 제4조에서 허용할 수 있을 것이다.

법제현황			특징
미국	개인정보 보호법제	공공 부문 연방프라이버시법, 전자통신프라이버시법 (Electronic Communications Privacy Act ECPA), 컴퓨터연결과 프라이버시보호법, 운전자프라이버시보호법(Driver's Privacy Protection Act of 1994) 등	개인정보를 포괄적으로 보호하는 법률의 제정 없이 특정유형의 정보조사 및 사용기관만을 규율, 독립된 위원회 등을 통한 보호가 아닌 개개인의 사법적 구제책에 의존
		민간 부문 공정신용기록법(Fair Credit Reporting Act), 소비자신용기록개혁법(Consumer Credit Reporting Reform Act), 금융기록프라이버시법(Financial Records Privacy Act), 전자자금이체법(Electronic Funds Transfer Act), 공정신용청구법(Fair Credit Billing Act), 공정채무수집법(Fair Debt Collection Act), 공정신용기회법(Equal Credit Opportunities) 등	
	생체	공공 부문 Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 1998년 신원절도법	9.11테러 이후 국가적인 안보를

법제현황			특징
정보 보호 법 제		(Identity Theft and Assumption Act of 1998), 국경보안강화및비자개혁법(Enhanced Border Security and Visa Entry Reform Act, 2002), 애국법(USA-PATRIOT ACT), 항공안전법(The Aviation Security Act Of 2001), 연방첩보감시법(The Federal Intelligence Surveillance Act) 등	강화하기 위한 목적으로 테러리스트 등 범죄자 감시의 강화
	민간 부문	금융프라이버시법, 공정채무수집법(Fair Debt Collection Practices Act), 금융현대화법 등	금융산업 관련 법률이 중심, 생체인식정보의 수집과 전달에 대한 포괄적 규율 미흡

※ 표는 김일환, 생체정보보호법제 정비방안에 관한 고찰, 토지공법연구 제33집, 361~362에서 직접 인용.

Ⅲ. 각 주(州)의 입법동향

1. 서

미국의 경우 원래 개인데이터 보호제도가 EU만큼 엄격하지 않았다는 배경이 있어 바이오매트릭스에 대해서도 EU에서와 같은 체계적·조직적인 움직임은 없다. 그러나 개별적으로 가이드라인의 책정¹¹⁾이

11) 국제바이오정보그룹(International Biometric Group: IBG)은 바이오매트릭스 시큐리티에 관한 미국 기업에 지나지 않지만, 바이오매트릭스의 프라이버시 혹은 개인데이터 보호의 문제에 관해서 “BioPrivacy Initiative”이라는 프레임워크를 제시하고 있다. 그 중에서도 “BioPrivacy Best Practices”라는 프라이버시보호 가이드라인이 주목받고 있다. 이는 프라이버시보호를 목적으로 한 Best Practice이나, 매우 상세한 내용을 담고 있으며 다음과 같은 25개 항목을 규정하고 있다. 즉, 「1. 범위의 한정, 2. 보편적인 고유 식별자의 작성에 대해서, 3. 바이오매트릭스 정보보유의 한정, 4. 잠재적인 시스템성능의 평가, 5 무관계인 정보의 수집 또는 정보의 보호, 8. 조회·판정 결과의 보호, 9. 시스템에의 액세스 제한, 10. 바이오 매트릭스 정보의 분리, 11. 시스템의 종료, 12. 「등록거부」의 자유, 13. 바이오매트릭스에 관계되는 정보의 수집 및 액세스, 14. 익명에 의한 등록, 15. 제3자에 의한 책임, 감사 및 감독, 16. 감

나, 몇 개 주(州)에서의 입법 등이 있다.¹²⁾

2. 각 주(州)의 입법 동향

Texas 주는 주법(Texas Statute Government Code) 제560장을 통하여 “바이오매트릭 신원확인요소는 망막(retina), 홍채(iris)패턴 · 지문 · 음성 · 손바닥형상 · 얼굴형을 대상으로 한다”고 규정하고 있다. 그리고 제 560.002조 바이오매트릭 신원확인요소의 공개에 대해서 “개인의 바이오매트릭 신원확인요소를 보유하는 정부기관은 본인의 동의 없이 바이오매트릭 신원확인요소를 매매 · 임대 또는 제3자에게 공개해서는 안 된다. 또한 바이오매트릭 신원확인요소가 누설되지 않도록 상당히 주의하여 보관 · 전송하여야 한다”고 규정하고 있다.¹³⁾

Illinois주의 경우 ‘바이오매트릭 정보 프라이버시법’(Biometric Information Privacy Act of 2008)은 제10조 정의에서 ‘바이오매트릭 신원확인요소’(Biometric Identifier)는 망막 혹은 홍채 스캔, 지문, 성문(voice-print), ‘손과 얼굴의 지형도’(hand or face geometry)의 스캔을 대상으로 한다고 규정한다. 그리고 제15조 보유(retention) · 수집(collection) · 공개(disclosure) · 파괴(destruction)에서 “바이오매트릭 신원확인요소나 바이오매트릭 정보(information)를 보유한 사적 기관은 대중에 공개된 정책

사 데이터의 완전한 공개, 17. 시스템 목적의 공개, 18. 등록의 공개, 19. 매칭의 공개, 20. 바이오매트릭스정보의 이용에 관한 공개, 21. 선택적 · 의무적 등록의 공개, 22. 시스템의 관리 · 감독 책임자의 공개, 23. 등록 · 인증 절차의 공개, 24. 바이오매트릭스 정보보호 및 시스템보호의 공개, 25. 삭제절차의 공개」가 바로 그것이다.

12) 자세한 것은 박정훈, 바이오매트릭스의 이용에 따른 법적 과제, 경희법학 제47권 제4호 (2013), 411면 이하 참조.

13) 「Government. Code Chapter 560. Biometric Identifier」, Acts 2003, 78th Leg., ch. 1275 renumbered V.T.C.A., Government Code § 559.001; Sec. 560.001 of Texas Government Code Ann. Chapter 560.

<http://www.statutes.legis.state.tx.us/DocViewer.aspx?K2DocKey=odbc%3a%2f%2fTCAS%2fASUPUBLIC.dbo.vwTCAS%2fGV%2fS%2fGV.560%40TCAS2&QueryText=biometric%3cOR%3eidentifier&HighlightType=1>.

을 가지고 있어야 하고, 초기 보유목적이 만족되었거나 3년의 기간을 한계로 보유기간과 영구적 삭제일정에 대한 지침을 설정해 두어야 한다. 관할법원에서 발부한 유효한 영장(warranty)이나 소환장(subpoena)이 없는 한, 사적 기관이 보유한 바이오메트릭 신원확인요소나 정보는 설정된 보유기간과 파기지침을 준수하여 처리되어야 한다”고 규정하고 있어 생체인식정보(biometric data)를 엄격하게 보호하는 법률을 보유하고 있다.

New Jersey주도 Illinois주와 마찬가지로 생체인식정보를 엄격한 보호하는 바이오메트릭식별자 프라이버시법(Biometric Identifier Privacy Act)의 제정을 2002년과 2006년에 시도하였으나 회기만료에 의한 법안자동폐기로 입법에 성공하지 못한 바 있다.¹⁴⁾ 캘리포니아·노스다코타·위스콘신·미주리 등 4개주 법률에서는 고용자들(employers)이 근로자들(employees)에게 피부아래에 삽입하여 식별정보(identifying information)를 전송하는 마이크로칩들의 사용을 강제하지 못하도록 규정하고 있다. 그러나 이들 법은 근로자들의 자발적인 마이크로칩의 장착을 금지하는 것은 아니다.¹⁵⁾ 이상과 같이 미국에서는 민간부문에서의 개인정보보호가 ‘자율규제’를 원칙으로 하고 있기 때문에 바이오메트릭스에 대해서도 자율규제를 전제로 가이드라인을 마련하는 경향이 일반적이다.

IV. 결 - 활용과 보호의 조화

14) Biometric Identifier Privacy Act, <http://www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM>.

15) Cal. Civ. Code § 52.7 (West 2009); Mo. Rev. Stat. § 285.035 (2008 Supp.); N.D. Cent. Code § 12.1-15-06 (2009); Wis. Stat. § 146.25 (2009).

일본의 생체정보 관련 법제 동향

강 영 기
(고려대 법학전문대학원 연구교수)

1. 생체정보의 정의

- 법령에서 직접 규율하고 있는지? 그 내용은?

일본의 2015년 개인정보보호법 개정에서는 개인정보의 정의를 명확히 한다는 취지에서 “개인 식별부호”라는 카테고리가 새로 마련되었다. “개인 식별부호”란 특정 개인의 신체 일부의 특징을 전자계산기용으로 제공하기 위해 변환시킨 문자, 번호, 기호 기타 부호로서 당해 특정 개인을 식별할 수 있는 것 중에서 정령으로 정하는 것(개인정보보호법 제2조2항1호)을 가리킨다. 그리고 이 “개인 식별부호”에 포함되는 것으로서 생존하는 개인에 관한 정보는 “개인정보”로서 법률의 보호를 받는다(동법 2조1항2호).

예컨대 “지문인증데이터”는 지문이라는 특정 개인의 신체 일부의 특징을 컴퓨터에서 이용하기 위해 변환시킨 문자, 번호, 기호 기타 부호로서 지문은 사람마다 다르기 때문에 당해 특정 개인을 식별할 수 있는 데이터라 할 수 있을 것이다. 여기서 “특정 개인을 식별”한다는 것은 “일반인의 판단력과 이해력을 가지고 생존하는 구체적인 인물과 정보와의 사이에 동일성을 인정하는데 이르는 것”을 말한다(瓜生和久編著, 「一問一答 平成27年改正個人情報保護法」, 12面). 간단히 말해서 지문의 주인이 다른 사람이 아니고 특정의 누구인지 알 수 있는 상태가 되면 특정 개인을 식별한 것이 된다. 실제로 법 개정의 논의가 중의원에서 이루어졌을 당시인 2015년3월25일 담당대신의 답변에서도 “개인 식별부호”의 예로서 지문인식 데이터가 상정되어 있었다.

이와 마찬가지로 컷구멍 모양의 인식데이터라도 그것이 특정 개인을 식별할 수 있는 것이라면 “개인 식별부호”에 해당될 수 있을 것이다.

한편 개정법에 따르면 “개인 식별부호”에 해당하는지 여부는 최종적으로 정령에서 정하도록 하고 있는데, 이에 포함되는 개인정보를 일정한 규칙에 따라 정리함으로써 특정한 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성된 정보의 집합물로서 목차, 색인 기타 검색을 용이하게 하기 위한 것을 가진 것을 가리킨다고 하고 있다(개인정보의 보호에 관한 법률시행령 1조).

물론 개정 전의 법률에서도 개인을 식별할 수 있는 귀 인증데이터는 개인정보에 포함될 수도 있다고(宇賀克也, 『個人情報保護法の逐条解説(第4版)』, 28面) 보았기 때문에 갑자기 생체정보가 개인정보에 포함되게 된 것이라고 볼 것은 아니다.

그럼 생체정보(biometrics)가 법률에서 말하는 개인정보에 해당한다면 그 관리는 어떻게 되어야 바람직할 것인가.

생체정보의 특징으로서는 이른바 나이를 먹어감에 따른 변화를 제외하면 정보 그자체가 크게 변하지는 않을 것이다. 따라서 생체정보가 한번 복제되면 줄곧 그것을 이용할 위험이 발생한다. 그러므로 생체정보는 다른 다양한 개인정보에 비해서 민감한 정보라고 할 수 있다. 결국 정보를 취급하는 사업자로서도 안전관리조치(정보보안조치)가 한층 중요해질 것이다. 안전관리조치의 내용으로서는 ①조직적인 조치 ②인적인 조치 ③물리적인 조치 ④기술적인 조치로 정리되고 있는데(瓜生和久, 前掲書, 69面; 第二東京弁護士会情報公開個人情報保護委員会編 『Q&A 改正個人情報保護法: パーソナルデータ保護法制の最前線』, 57面(数藤雅彦 執筆部分) 등 참조) 생체정보의 경우는 그 중요성에 비추어 이들 조치의 모든 면에서 높은 수준의 조치가 요구될 것이다. 아무튼 정보누설사건이 종종 발생하는 상황에서 생체인증(biometrics)의 정보보안을 어떻게 구축할 것인지는 사회로서도 사업자

로서도 정보의 주체인 본인으로서도 중대한 문제이므로 법제도와 해석론도 중요해질 것이다.

* 개인정보보호법 개정 포인트

(1) 개인정보의 정의를 명확화

1) 개인정보 정의의 명확화(2조1항·2항)

특정개인의 신체적 특징을 변환시킨 것(얼굴인식 데이터 등)은 특정 개인을 식별하는 정보이기 때문에 ‘개인식별부호’로서 개인정보로 하여 명확히 한다.

현행법에서는 개인정보의 정의에 애매한 점이 남아 있어서 비즈니스 상의 문제가 되는 경우가 많았는데, 개정법에서는 사업자가 퍼스널 데이터의 활용에 주저하지 않도록 ‘개인정보’의 범위를 명확히 하였다. 현행법의 제2조1항에 괄호를 사용하여 (다른 정보와 용이하게 조합하는 것이 가능하고 그에 따라 특정 개인을 식별하는 것이 가능한 경우를 포함한다)고 되어 있어 다른 정보와 조합하여 개인이 특정될 수 있는 경우는 개인정보로 되어 있고 이점은 개정 전후에 있어서 변함이 없다. 이번 개정으로 새로이 “개인식별부호”가 정의되고 이에 해당하는 정보가 개인정보라는 것이 명확해진다(2조1항1호). 개정법에 의하면 다음 2가지로 분류되는데(2조2항), ① 특정 개인의 신체 일부의 특징을 전자계산기용으로 제공하기 위하여 변환시킨 문자, 번호, 기호 기타 부호 ② 개인에게 제공되는 서비스의 이용 혹은 개인에게 판매되는 상품의 구입에 관하여 배정되거나 또는 개인에게 발행되는 카드 기타 서류에 기재되거나 혹은 전자적 방식으로 기록된 문자, 번호, 기호 기타 부호로서 그 이용자 혹은 구입자 또는 발행을 받는 자마다 다른 것으로 되도록 배정되거나 또는 기재되거나 혹은 기록됨으로써 특정 이용자 혹은 구입자 또는 발행을 받는 자를 식별할 수 있는 것.

개정법에서는 “정령으로 정하는 것을 말한다”고 되어 있고, 구체적인 확정은 정령의 내용에 따르겠지만 ①은 생체인증 등에 사용되는 지문, 홍채, 정맥인식 데이터 등 개인의 신체적 특징을 디지털화한 정보 등이고 ②는 면허증 번호, 여권번호나 포인트 카드의 회원번호 등이 해당될 것이다.

2) 배려가 필요한 개인정보(2조3항)

본인에 대한 부당한 차별 또는 편견이 생겨나지 않도록 인종, 신조, 병력 등이 포함되는 개인정보에 대해서는 본인동의를 얻어 취득하는 것을 원칙적으로 의무화하고, 본인동의를 얻지 않은 제3자 제공(opt-out)을 금지한다.

3) 개인정보 데이터베이스 등의 제외(2조4항)

개인정보 데이터베이스 등에서 이용방법을 보고 개인의 권리 이익을 해할 염려가 없는 것에 대해서는 제외한다.

<참고> 준(準)개인정보의 구체적 사례

- 제7회 personal data에 관한 검토회의 자료에서 제시된 바에 따르면,
- ① 여권번호, 면허증번호, IP주소, 휴대단말기의 ID 등 개인 또는 개인의 정보
통신단말기 등에 매겨져 계속적으로 공용되는 것
 - ② 얼굴인식데이터, 유전자정보, 음성의 특성, 지문 등 개인의 생체적 신체적 특성에 관한 정보로서 보편성이 있는 것
 - ③ 이동이력, 구매이력 등의 특징적인 행동의 이력

>> “준(準)개인정보에 포함되는 구체적 항목”에 관한 보다 구체적인 내용은 ‘퍼스널 데이터에 관한 검토회’의 ‘기술검토 Working Group 보고서’ “(가칭)준개인정보 및 개인특정성 저감 데이터에 관한 기술적

관점에서의 고찰에 대하여”(2014.5)에 나와 있는데, 이에 의하면 특히 개인의 신체적 특성에 관한 것(대체로 생체정보에 해당하는 것으로 판단됨)에는 지문, 성문(聲紋), 정맥 패턴, 홍채, DNA, 얼굴인식 데이터, 손바닥 모양, 생체인증에서 사용되는 데이터(생체인증방식 고유의 방법으로 수치화한 데이터도 포함하고, 얼굴화상인식 데이터도 포함), 보행 패턴, 필적, 성별, 피부색, 인종, 가족구성, 혈액형, 머리카락색깔, 혈압, 맥박, 신장, 체중 등이 있다.

(2) 개인정보이용을 위한 조치

1) 익명가공정보(2조9항·10항, 36조-39조)

특정 개인을 식별할 수 없도록 개인정보를 가공한 것을 ‘익명가공 정보’로 정의하고 그 가공방법을 정함과 동시에 사업자에 의한 공표 등 그 취급에 대해서 규율을 마련한다.

2) 이용목적 제한의 완화(15조2항)

개인정보를 취득한 때의 이용목적에서 새로운 이용목적으로 변경하는 것을 제한하는 규정을 완화한다.

3) 개인정보보호지침(53조)

인정개인정보보호단체가 개인정보보호지침을 작성하는 때에는 소비자의 의견 등을 청취함과 동시에 개인정보보호위원회에 신고를 하고 개인정보보호위원회는 그 내용을 공표한다.

(3) 개인정보보호의 강화

1) 소규모취급사업자에 대한 대응(2조5항)

취급하는 개인정보가 5000명 분 이하인 사업자에게도 본법을 적용한다.

2) Opt-out 규정의 엄격화(23조2항-4항)

opt-out규정(본인동의를 얻지 않은 제3자 제공의 특례)에 의한 제3자 제공을 하려는 경우, 데이터 항목 등을 개인정보보호위원회에 제출하고 개인정보보호위원회는 그 내용을 공표한다.

3) Traceability의 확보(25조 · 26조)

수령자는 제공자의 성명과 데이터 취득경위 등을 확인·기록하고 일정기간 그 내용을 보존한다. 제공자도 수령자의 성명 등을 기록하고 일정기간 보존하여야 한다.

4) 데이터베이스 제공의 죄(83조)

개인정보 데이터베이스 등을 취급하는 사무에 종사하는 자 또는 종사하고 있던 자가 부정한 이익을 도모할 목적으로 그 개인정보 데이터베이스 등을 제3자에 제공하거나 또는 도용하는 행위를 처벌한다.

5) 개인정보보호위원회(50조-65조)

내각부의 외국(外局)으로서 개인정보보호위원회를 신설(번호법의 특정개인정보보호위원회를 개조)하고 현행 주무대신이 가지는 권한을 집약함과 동시에 출입검사의 권한 등을 추가한다.

6) 외국사업자에 대한 제3자 제공(24조)

개인정보보호위원회의 규칙에 따른 방법, 또는 개인정보보호위원회가 인정한 국가 또는 본인동시에 의해 외국사업자에 대한 제3자 제공이 가능하다.

7) 국경을 초월한 적용과 외국집행당국에 대한 정보제공(75조, 78조)

물품과 서비스의 제공과 더불어 일본 거주자 등의 개인정보를 취득한 외국의 개인정보취급사업자에 대해서도 본법을 원칙적으로 적용한

다. 또한 집행에 있어서 외국집행당국에 대한 정보제공이 가능한 것으로 한다.

8) 공시, 정정, 이용정지 등(28조-34조)

본인에 의한 공시, 정정, 이용정지 등의 요구는 재판소에 소를 제기할 수 있는 청구권이라는 것을 명확히 한다.

2. 관련 분야에 대한 현황 및 사례

-활용의 측면 및 보호의 양 측면에서 소개 필요

(1) 활용의 측면 중심

1) Toshiba와 일본 IBM이 생체정보를 활용한 자동차운행관리 솔루션분야에서 협력

2015년 5월 14일 주식회사 Toshiba와 일본 IBM은 양사의 기술을 융합하여 drive recorder나 GPS 등의 종래의 정보에 운전자의 생체정보를 더하여 안심·안전·에너지절감 등의 실현을 위한 자동차운행관리 솔루션분야에서 협력하기로 하였다. 여기서는 drive recorder나 헨 등의 정보에 운전자의 건강상태와 생체정보를 추가하고 수집된 데이터를 해석하여 그 결과를 보다 안전하고 에너지절감으로 이어지는 운행관리 솔루션 개발에 활용하려는 것이다. 개발된 서비스는 운송회사나 택시회사, 보험회사 등 다양한 기업들에 제공될 것이다. 그러므로 지금까지의 운행관리 솔루션에서는 차량에 특화된 것이 대부분이었지만, 고품질의 솔루션을 제공하기 위해서는 drive recorder나 날씨, 교통상황은 물론, 운전자의 건강상태와 생체정보 등 광범위한 데이터가 필요해진다.

2) 소프트뱅크와 공동개발사업을 전개하는 FiNC가 개인생체정보를 활용한 헬스케어서비스 개발 도모

주식회사 핑크(FiNC)는 헬스케어의 예방영역에서 서비스를 제공하는 기업으로서 생활습관의 지도, 유전자검사 등을 이용한 여러 가지 헬스케어서비스의 기획과 개발을 통해 운영하고 있다. 2012년 4월 설립되었으며 당시에는 DNA와 혈액, 생활습관 등을 조사하는 유전자검사 서비스를 제공하였으나 검사만으로는 이용자에게 정보를 제공하는 것 이상의 support를 할 수 없다는 판단아래, 사업방향을 변경하고 온라인상의 트레이너나 관리영양사의 지도를 받을 수 있는 다이어트프로그램을 고안하였다. 그리고 2014년 3월 유전자검사 결과를 토대로 다이어트 support를 받을 수 있는 웹 프로그램(당시는 REPUL현재의 FiNC 다이어트 가정교사(<https://finc.co.jp/portfolio/finc-diet-coach/>))을 공개하였다. 이것은 이용자가 웹 사이트상에서 매일의 식사 동영상과 체중을 업로드 함으로써 영양사 등 전문가의 지도를 받을 수 있는 서비스이다. 즉, FiNC 앱(App)은 유전자와 혈액정보 등 생체정보를 이용하여 각 이용자에게 헬스케어콘텐츠를 Recommend하는 퍼스널 코치 애플리케이션이다. 여기서 는 날마다의 식사와 체중, 운동의 진척상황을 공유하는 등 이용자 간의 연계를 통해 혼자서는 지속하기 어려운 다이어트와 생활습관의 개선을 촉진시킨다. 그리고 FiNC는 2015년 10월 헬스케어서비스인 ‘퍼스널 신체 support’를 소프트뱅크와 공동개발하기로 한 내용을 발표하고 IBM의 인공지능 IBM Watson(<http://www.ibm.com/smarterplanet/jp/ja/ibmwatson/>)을 활용하여 퍼스널데이터에 기초한 고품질의 헬스케어서비스를 제공하기로 하였다.

의료비의 증가, 저 출산 고령화, 인구감소, 경제축소 등의 세계 공통의 과제상황 속에서 어느 국가도 명확한 해결책을 제시하지 못하는 상태인데, FiNC가 이용자의 생체정보 등 생활데이터를 토대로 복합적

인 분석을 하고 각 이용자에게 건강을 위한 정보제공을 실시하고 현역의사, 약제사, 관리영양사, 트레이너, 엔지니어 등이 힘을 합쳐 웹과 스마트 디바이스 등을 활용하여 이용자에게 퍼스널 정보를 제공함으로써 세계최초로 해결책을 도출하겠다는 의지를 표명하는 것은 유의미한 일이라 평가된다.

(2) 보호의 측면 중심

퍼스널 데이터의 프라이버시 보호 실현을 위한 익명화 기술

1) 익명화기술의 등장 배경

빅 데이터 분석과 향후의 사물 인터넷(IoT)의 발전에 따라 데이터는 더욱 증가할 것이고 수집된 데이터를 퍼스널데이터로서 활용하고 새로운 비즈니스 기회의 창출이 기대될 것이다. 한편, 사이버 공격과 내부부정에 의한 대규모의 개인정보 유출, 프라이버시에 대한 배려가 없는 서비스의 중지 등의 사례도 발생하고 있다. 그리고 My Number 제도와 개인정보보호법의 개정, EU 데이터 보호규칙 등 법적 규제도 강화되는 경향에 있는데, 후지쯔 연구소에서는 이들 법안과 규제에 준거한 프라이버시 정보를 익명화·암호화하는 기술을 개발하고 있다. 여기서 개발한 것이 k-익명화 등 익명화기술이다.

2013년 7월 JR동일본 전철주식회사가 Suica의 승차이력 데이터를 익명화하여 판매하고자 한 사례가 있는데, 사업자에 대해 많은 이용자로부터 반대하는 의견이 많아서 사실상 서비스를 정지하였다. 이러한 영향으로 퍼스널데이터의 취급에 관한 규율을 명확히 하기 위해 내각 IT 종합전략본부는 ‘퍼스널데이터에 관한 검토회’를 설치하고 2014년 6월에 ‘퍼스널데이터의 활용에 관한 제도개정대강’을 만든 다음에, 2015년 개인정보보호법이 개정되어 2017년에 시행될 예정이다.

개정된 개인정보보호법은 많은 특징이 있지만, 그 중에서도 퍼스널 데이터를 ‘익명가공정보’로 가공하고 일정한 제약(데이터제공 상대방에서 데이터로부터의 개인 재특정 금지)아래 본인의 동의가 없이도 데이터를 제3자에게 제공할 수 있는 점이 큰 특징이다. 익명가공정보는 특정 개인의 식별은 물론, 복원될 수 없도록 가공된 정보이다. 이러한 가공의 실현을 위한 기술로서 익명화기술이 주목되고 중요도가 점차 커질 것이다.

2) 익명화 기술의 개요

익명가공정보로 가공하는 데는 여러 가지 수법이 사용되지만, 익명가공정보를 생성하는 수법에 요청되는 익명가공기준에 대해서는 분야마다 개인정보보호위원회가 향후 책정할 것이라고 한다. 익명화기술로 불리는 개인을 특정할 수 없도록 데이터를 가공하는 기술이 유력한 후보로 떠오르고 있는데, 익명화기술에 대해서는 과거에도 많은 연구가 있었지만 여기서는 대표적인 2가지 기술과 후지쓰의 익명화기술에 대해서만 소개한다.

① 가명화

실명을 가명으로 바꿈으로써 개인의 특정을 방지하는 것으로서, 가명화한 후에도 동일인물의 건강상태의 경과를 추적할 수 있는 장점이 있지만, 성별이나 연령 등 간접적으로 개인을 특정할 수 있는 속성의 조합으로 기록에 대응하는 개인을 특정할 가능성이 있다는 점이 단점이다.

② k-익명화

k-익명화 기술은 간접적으로 개인특정 가능한 속성을 준(準)식별인자(QI:Quasi-identifier)로 정의함으로써 동일한 QI의 조합이 반드시 k명 이상 존재하도록 데이터를 가공하고 기록에 대응하는 개인특정을 방지한다.

③ 후지쯔 연구소의 익명화기술

후지쯔 연구소에서는 익명화 실현을 위한 기술로서 정보 Gate Way 기술과 k-익명화 라이브러리를 개발하였다.

정보 Gate Way는 클라우드 등 조직외부의 서비스를 이용할 때 정보 Gate Way를 사이에 두고 외부와 데이터를 주고받음으로써 외부서비스에서는 본래의 데이터를 알 수 없도록 숨기고, 이용 시에는 숨겨진 데이터를 본래의 데이터로 복원할 수 있다. 숨길 때 가명화를 이용함으로써 정보 Gate Way로 일괄 처리하고 기존 시스템에 대한 수정을 최소한으로 억제한다.

한편, k-익명화 라이브러리의 개발에 성공하였는데, 독자적인 k-익명화 알고리즘을 개발함으로써 주기억장치가 읽는 데이터의 크기를 입력데이터보다 작게 할 수 있어서 탑재메모리가 작은 옴가의 컴퓨터로도 속도가 빠른 k-익명화 처리가 가능하다. 또한 이 라이브러리에는 k-익명화보다 고도의 프라이버시보호를 실현하는 기능이 탑재되어 있어서 프라이버시정보의 누출이 방지된다.

위에서 말한 정보 Gate Way와 k-익명화 라이브러리를 탑재한 익명화 솔루션으로서 후지쯔는 NESTGate를 제품화하였다. NESTGate를 활용하면 가명화, k-익명화 처리, 통계법 가이드라인¹⁾ 등 각종의 익명화 처리가 가능하다고 한다.

3. 기타 중요하다고 생각하는 점

일본 개인정보보호법의 개정은 많은 변화가 있어서 실제로 개인정보를 취급하는 업무현장에도 다양한 영향을 미칠 것으로 보인다. 그리고 개정법의 구체적인 내용은 정령과 2016년 1월에 발족한 개인정

1) 총무성, 익명 데이터의 작성·제공에 관한 가이드라인, 2011.3.28.

보보호위원회가 정하는 규칙(가이드라인)에 의한 부분이 많아서 불명확한 부분이 많은 것이 사실이다. 예컨대, 익명가공정보에 대해서도 익명가공정보를 작성하는 때는 개인정보를 복원할 수 없도록 개인정보보호위원회 규칙으로 정하는 기준에 따라 개인정보를 가공하는 것이 강제되지만, 모든 개인정보를 익명화할 수 있는 수단은 존재하지 않고 익명가공정보의 취급에 관한 감독에는 한계가 있다는 지적도 있다. 만일 기준이 너무 엄격하거나 혹은 애매하거나 하면 익명가공정보는 사용되지 않을 수도 있으므로 동향을 주시할 필요가 있다. 개정법의 시행이 공포일부터 2년 이내로 되어 있고 늦어도 2017년 9월까지 시행되므로 그때까지 기업들은 자신에 대한 영향분석과 대응방안을 충분히 검토할 필요가 있을 것이다.

사실 개인정보보호법안은 예금계좌에도 My Number를 붙이는 번호법의 개정법안과 일괄적으로 심의되었는데, 2016년 1월부터 시행된 My Number제도에 비하여 주목을 크게 받지 못하는 못하였다. 내각부가 2015년 11월에 발표한 ‘개인정보보호법의 개정에 관한 여론조사’에서 개인정보보호법의 개정에 대한 인지도가 매우 낮았다는 결과가 나왔다. 그런데 이번 법개정은 개인정보를 ‘익명가공’한 정보를 기업 등에게 제공할 수 있도록 하고 상품의 구매이력 등의 퍼스널 데이터를 경제활동에 활용할 수 있도록 하는 내용 등 중요한 항목이 포함되어 있다. 퍼스널 데이터의 활용은 일본정부의 성장전략의 일환으로 진행된 것인데, 일정한 규율기준이 만들어짐으로써 빅 데이터의 분석 등 정보의 활용이 촉진되고 산업진흥과 국제경쟁력 향상에도 기여할 수 있을 것이다. 기업의 경쟁력은 다양한 채널로부터 수집된 정보를 얼마나 빨리 비즈니스의 기회로 만드는가에 달려있다. 또한 퍼스널 데이터 등의 활용이 활발해지는 만큼 관리상의 리스크도 커질 것이므로 이에 대한 대책과 관련한 개인정보관련 보험과 정보보안체제의 정비도 함께 이루어지는 것이 자연스런 움직임이 될 것이라 본다.

토 론 문

토 론 문

손 형 섭
(경성대학교 법정대학 조교수)

I. 들어가며

1. 생체정보의 개념

생체정보 활용도 이용자가 안심하고 활용할 수 있는 정보가 되도록 노력해야 한다.

생체정보의 개념 정의에서부터 연구 범위가 크게 달라진다. 생체인식정보로 개념을 협의로 정할 것인지 문제이다. 따라서 이 연구에서 생체정보에 대한 협의 광의로 구별하여 연구의 포커스를 맞추어야 한다. 즉, 의료정보는 광의의 문제이고 협의의 생체정보 연구를 생체인증을 중심으로 논의하면 좋을 것이다.

또한 생체정보가 민감정보인가 아닌가의 문제에 대하여 법령에 언급을 할 필요가 있다. 즉 민감하지 않은 생체인증 방법이 가능한 법규 규정이 필요하다.

2. 앞으로의 전개

아직 생체정보의 국내 산업으로는 매출액 규모가 매우 작다. 따라서 제사회의 표준을 만든 것으로 접근해야 할 것이다. 이 미국과 일본에서는 생체정보 활용을 위한 높은 기술을 활용하고 있다.

최근 일본에서는 은행 APM기계에 指靜脈인증을 선택할 수 있게 하고 있고, 얼굴 인증에 관한 NEC의 기술력도 세계적인 수준이다.

공공과 민간도 다른 양상으로 논의되어야 한다. 이용의 활성화와 규율이 논의되어야 한다.

3. 검토되어야 할 법령들

- 대한민국헌법
- 개인정보보호법과 개별법과의 관계 문제
- 바이오정보 가이드라인 행자부 개정예정
- 정보보호산업 진흥에 관한 법률
- 정보통신망법 시행령 2013
- 제15조 바이오 정보(종래 일방향 암호화를 요구했다가 이를 삭제)
- 전자금융감독규정 2015.3.18.
- 공인인증서사용의무 폐지 제37조 1항~3항
- 공인인증서 비밀번호를 지문으로 대체하는 서비스 시험 중
- 금융감독위원회 - 금융은 변경해서 ---
- FIDO(Fast IDentity Online) 얼라이언스(Alliance) 표준
- 금융결제 Bio정보- 서버에 전송되지 않고 서부에서 fintech
- 핀테크

4. 쟁 점

- (1) 원본정보도 일체 암호화해야 하는 가 문제
- (2) 계약에 의해 허용 가능한 범위
 - 자율규제(이상경 교수님)
- (3) 지문, 입술 모양, DNA

생체정보 - 전자서명 / 보험법 전자서명 가능 그러나 타인을 위한 생명보험 가입 시에는 타인의 동의를 받아야 한다. 상법 701조 반듯이 실명 동의를 받아야 한다. 아직은 위변도가 가능하고 범죄에 악용

될 수 있다는 반대 논지. 19대 국회. 20대 시작부터 개정하기 위한 입법노력이 있다.

특별법과의 관계 상충의 문제를 어떻게 해결할 것인가도 문제이다.

* (확인요망) 일본은 동의를 받으면 되고 서면이나 전자이나 무방하다.
개인정보보호법 제6조 다른 법이 우선한다(김일환).

II. 비교검토

1. 독일

- 2006년 김일환 교수님 독일 생체인증정보 자료
- 생체인증(Biometrie), 생체인증정보(Biometrische Daten)
- 정보보호와 활용
- 2001년 9.11 테러 이후 유럽연합의 테러행위 공동대처를 위해 생체정보 활용 시작
- 외국인체류법, 난민법 규정
- 여권법
- 개인신분증법 - 사진과 지문, 생체정보 일부 규정
- 외국인체류법
- 2004 전자서명법
- 95/46 개인정보지침
- 2016년 정보보호 기본규칙
- 정보자기결정권, 민감정보 문제 - 유럽 정보보호 기본규칙 제9조
 - * 생체정보 수집, 처리를 위해 특별한 법적 근거를 필요로 하며 특별한법이 없으면 연방개인정보보호법에 의해 처리함
- BDSG - 6조에서 동영상 정보 규정
- 여행자여권 생체정보 저장 허용문제 - 헌법소원 각하

- 홍채인식 -
- 공공부문에서의 생체정보 문제를 중심으로 발표함.
- 민간에서 이용 가능성 문제가 논의되어야 함
- 각 국가의 개인정보보호법에 따라 민간의 생체정보의 이용과 활용에 차이가 날 것임(김일환)

2. 일 본

- 2015년 개인정보보호법 개정을 통하여 개인식별부호: 생체정보가 포함될 수 있게 되었다.
- 개인정보의 정의 명확화: 용이조합가능성 정보도 포함
- 개인식별부호
- 준개인정보 2013. 5. 大綱 / 2013. 10. 보고서에서 준개인정보 규정
- 활용을 위한 보호장치는 - 익명가공정보 - 완화
- 개인정보보호지침
- 익명화기술- k-익명화- 후지쯔 익명화기술의 선두주자임
- 1월 특정개인정보보호위원회가 개인정보보호위원회의 변경 발족
- 지문인증 데이터
- 생체정보의 불변성 문제: 유출되면 큰 부작용이 우려: 기본적인 보호는 필수

3. 프랑스

- 생체인식
- “생체정보 권력”
- EU 디렉티브 공공, 민사에서도 활용
- 여권
- 1978년 정보 문서 자유법 -

- 홍채 인식, 지문 등 예시
- 민감한 개인정보: 공정성 비례의 원칙 사전 동의: 정보자유위원회
- 보안전자국민신분증
- 전자여권
- 민사관계 격지자, 집단간 계약에서의 신원확인 문제
- 전자서명을 위한 법제 정비 중, 암호화 하여 전송 등
- 생체인식 기여할 듯
- 생체정보 여권 : 지문수집
- 외국인 입국 및 체류와 망명권 법적: 외국인 생체정보 저장 보존
- 조세법전

의료정보를 처방전 포함한 의료기록을 저장하고 건강보험기관에 정보를 전송하고 있다. 금액 지급만을 정보로 남고 있고 질병명 등까지 남는 것은 아니다.

4. 미 국

- 미국의 연방법 - 생체정보의 활용
- 6부처에 관련 연방상무부의 국가표준기술원 : 측정, 평가, 표준 (standards)에 집중하고 있다.
- 추적자료
- 국방부
- Real ID 테러를 막고 위조변조를 감소시키기 위한 노력 : a notice of proposes rulemaking(NPRM) 하고 있다.
- 그동안 연방차원에서 SS card만 있다.
- 생체인식관리사무국 (OBIM)
- 프라이버시권에 대한 guidance를 작성하고 있다.

- OBIM 은 US- VISIT를 위해 양손검지- 십지지문- 사진 활용
- TWIC 운송체계 위험 노출 막고 있다.
- 법적인 근거 만들고 있다.
- 등록자 여행프로그램 개발: 시장 주도적 프로그램: 등록된 여행자의 생체정보를 활용할 수 있도록 논의하고 있다.
- 연방수사국FBI 생체인식표준(Biometric standards)
- 통합자동지문인식체계(IAFIS)를 만들어 활용하려 하고 있다.
- 지문의 전자적 응답과 신원확인 위해 노력하고 있다.
- 생체인식특성화센터(the Biometric Center of Excellence BCOE)
- 프라이버시법 생체인식 전문가 등이 업무수행을 하고 있다.
- 미 국무부 전자여권(US Electronic Passport)
- 사진 안면인식 등 위조방지 보안을 위한 체계화
- 스마트카드 판독기 : 생체인식 진정증명을 위해 카드판독기로 식속 하게 일어날 수 있다. 상당히 식속하과 진보된 활용 방식
- 여러 가지 가이드라인
- 생체정보 활용에 대해서도 가이드라인 -
- Texas 생체인식정보 신원확인 요소: 신원확인 요소에 대하여 공개
- Illinois 주: 가장 엄격한 내용
- New Jersey 주: 근로자들이 몸에 식별정보를 전송하는 마이크로 칩 들을 장착하는 것도 가능하게 되는 움직임
- 미국은 메칭으로 생체정보를 활용하려고 하고 있다.
- 자율규제와 개인정보 활용과 보호

Ⅲ. 소 결

생체인증 문제는 꾸준히 기술적 법리적으로 연구되어야 할 문제이다. 생체정보에 관한 의료정보 문제도 큰 포션을 문제로서 다양하게 검토되어야 한다.

현재 FIDO Alliance가 국내는 물론 해외 기업에서 인증 강화되고 있다. FIDO Alliance는 최근 미국을 중심으로 온라인 인증의 강화 움직임에 따른 신표준을 확립하는 움직임이 확대되었고, 이 역할을 하는 사람은 FIDO Alliance라고 하는 단체로, 종래 페스워드와 유저명에 의한 인증을 대신하고 생체인증 등이 새로운 인증기술 보급 및 비전으로 제기하고 있다. FIDO Alliance에서는 공개 키 암호 방식에 근거하여 2가지 인증용 표준프로토콜을 책정하고 있다. 이 프로토콜의 하나가 다요소 인증을 하는 패턴을 상정한 U2F(Universal 2nd Factor: U2F)이다.

이에 대응하여 FIDO Alliance 프로토콜의 하나인 U2F에 대응한 CloudgateUNO 새 버전을 2015년 6월 20일에 새로 제공되기도 했다. 최근 하드 메이커, 소프트에 메이커에서 이 기준을 수용하고 있다.

FIDO Alliance의 준거인 서비스가 세계에 유통되고, 현재 급격히 증하되고 있는 공공의 피해를 해결하기 위한 시큐리티상의 모델로 정부와 미국정보의 IT 전문가들로부터 주목받고 2015년 6월에 미국 국립표준기술연구소(NIST)가 FIDO Alliance에 가입하여, 새로운 인증솔루션을 조기 도입하려 하고 있다.

이것이 일본에 2015년 11월 30일 FIDO Alliance에 대한 동경 세미나가 개최되었다. 일본의 각 기업이 FIDO 준거 제품을 구입하고 있다.

국내에서도 FIDO에 따른 제품들이 제공되고 있다. 앞으로 법제 연구에서는 FIDO Alliance의 내용을 일부 법에 두고 대부분은 시행규칙 및 가이드라인으로 수용하여 국내외 생체인증 및 생체정보 활용에 대한 공적인 규정 정립이 수행되어야 할 것이다.

제5차 워크숍
생체정보의 활용 및 보호를
위한 법제 정비방안

2016. 9. 26.

일 정

1. 목 적 : 생체정보의 활용 및 보호를 위한 법제 정비방안

2. 일 시 : 2016년 9월 26일(월) 09:00~12:00

3. 장 소 : 서울역 회의실 제2호

4. 세부일정

(1) 사 회

- 김일환(성균관대 법학전문대학원 교수)

(2) 연구개요 발표

- 김현희(연구책임, 한국법제연구원 연구위원)

(3) 발 표

- 김재성(한국인터넷진흥원 연구위원)

- 이은우(법무법인 지향 변호사)

(4) 토 론

- 이창범(김장 법률사무소 전문위원)

- 정필운(교원대 일반사회교육과 교수)

- 김현경(서울과기대 IT정책대학원 교수)

- 김주영(명지대 법학과 교수)

- 방동희(부산대 법전원 교수)

- 정소영(충북대 법전원 강사)

- 조용혁(법제연 법제전략분석실 부연구위원)

- 최경환(한국인터넷진흥원 책임연구원)

목 차

□ 발 제 문	253
○ 바이오인식시스템 보안위협과 차세대 Medical biometrics (김재성)	255
○ 생체인식 정보의 처리에 관한 개인정보 보호법제의 현황과 개선방향(이은우)	279
□ 토 론 문	295
○ 생체정보의 현황(패러다임 변화) 및 입법 전략에 대한 고찰 (방동희)	297

발 제 문

발 제 문 1

김 재 성
(한국인터넷진흥원 연구위원)

한국법제연구원 워크숍

바이오인식시스템 보안위협과 차세대 Medical biometrics

2016. 09. 26

공학박사 김재성 (Dr. Jason Kim, jskim@kisa.or.kr)
보안기술확산팀, ABC (아시아바이오인식협의회) 의장, TTA PG505 의장

KISA 한국인터넷진흥원
Korea Internet & Security Agency

발표순서

KISA 한국인터넷진흥원





- I** 바이오인식기술 변천사 및 국외동향
- II** 바이오인식시스템 보안취약점 및 대책
- III** 바이오인식기술 관련 KISA 대응현황
- IV** Medical Biometrics 기술현황 및 전망
- V** KISA 생체신호 인증기술 개발현황 및 향후계획

2016-09-26 한국법제연구원 워크숍


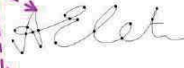


I 바이오인식기술 변천사 및 국외동향 – Definition

바이오인식이란?
 사람의 신체적(얼굴/홍채/지문/정맥 등), 행동적(음성/서명/자판/걸음걸이 등) 특징을 자동화된 IT 기술로 추출·저장해, 다양한 IT 기기로 개인의 신원을 확인하는 수단

신체적 특징 (Physiological Biometrics)

- ② 얼굴 (조명) 
- ③ 홍채 (원거리) 
- ① 지문 (위조) 
- ④ 정맥 (고령자, 계집) 
[손가락정맥] [손등정맥]

행동적 특징 (Behavioral Biometrics)

- [음성] (변조) 
- [서명] (정확성) 
- [키보딩습관] (직업유리) 
- [걸음걸이] (정확성) 

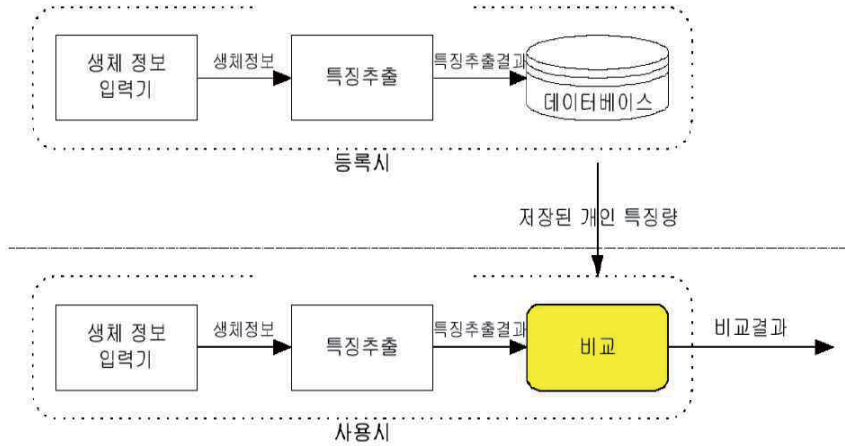
2016-09-26 1 한국법제연구원 워크숍

I 바이오인식기술 변천사 및 국외동향 – Modality

① 지문	<ul style="list-style-type: none"> ◎ 가장 오래 사용된(100년 이상) 바이오인식 종류 ◎ 임신 24주째에 생성되어, 평생 불변 ◎ 무지문증, 다한증 등으로 약 2% 정도는 지문 취득 불가 	
② 얼굴	<ul style="list-style-type: none"> ◎ 얼굴 외곽, 눈/눈썹/코모양, 눈/코/턱 간격 등 측정 ◎ 비접촉 방식으로 사용자의 거부감이 적음 ◎ 환경(안경, 가발, 조명 등) 영향이 많고, 인식 시간이 오래 걸림 	
③ 홍채	<ul style="list-style-type: none"> ◎ 홍채 모양, 색깔, 망막 모세혈관의 형태소 등 인식 ◎ 생후 18개월에 모양이 완성된 후, 평생 불변 ◎ 사용자 거부감이 높으며, 제품의 크기가 큼 	
④ 정맥	<ul style="list-style-type: none"> ◎ 손등 또는 손가락의 혈관 형태를 측정 ◎ 적외선 카메라를 이용, 혈관을 투시 후, 잔영을 인식 ◎ 하드웨어 구성이 복잡해, 제품 가격이 고가임 	

2016-09-26 2 한국법제연구원 워크숍

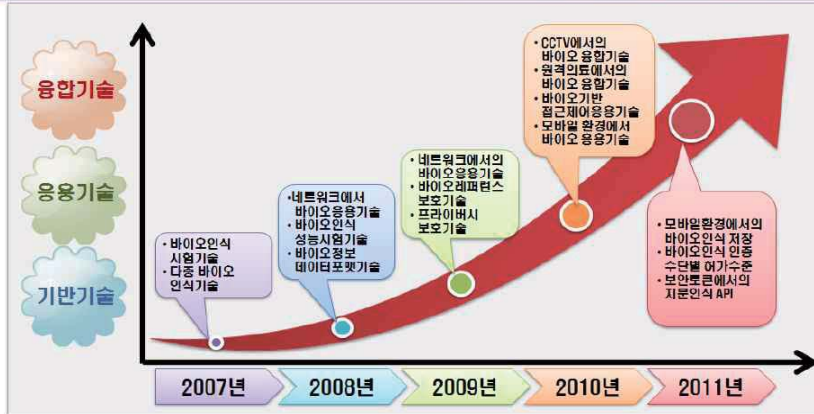
I 바이오인식기술 발전사 및 국외동향 – Biometric system



I 바이오인식기술 발전사 및 국외동향 – Trends

Worldwide (미국 01년 911 테러, 02.12 ISO/IEC SC37 발족, 06년 전자여권 도입, 12년 애플 □ 아이폰),

대면 & 비대면서비스로 전환됨에 따라 유연조어 강인한 New 융합인식기술이 요구됨



Korea (01년 KBA 협의체발족, 06년 KISA 시험센터발족, 08년 전자여권 발급/US-VISIT 무비자, 13년 삼성전자 갤럭시S)

I 바이오인식기술 발전사 및 국외동향 - China

Body
Face

Probe Image Rank 1 Rank 2 Rank 3 Rank 4 Rank 5

ABC2011, China Beijing 중산대학

2016-09-26

5

한국법제연구원 워크숍

I 바이오인식기술 발전사 및 국외동향 - UK

Image Sequence → Preprocess → Gait Trajectory Model → 3D Head Tracking → Frontal face Reconst. → Super Resol. Image

Preprocess: Silhouette extraction, BG subtraction, Homo. Calculation using SURF

Gait Trajectory Model: Gait model building, Model fitting using LM, Potential face region extraction

3D Head Tracking: Corresponding point detection, Motion vector calculation using LM

Frontal face Reconst.: View changing using 2D homo.

Super Resol. Image: HR image generation using SR methods

ABC2012, UK Southampton대학

2016-09-26

6

한국법제연구원 워크숍

I 바이오인식기술 발전사 및 국외동향 – Singapore

Handheld Scanners

Desktop Scanners

ABC2011, Singapore 장이공양

2016-09-26 7 한국법제연구원 워크숍

I 바이오인식기술 발전사 및 국외동향 – Mobile Biometrics

Smart Phone Touch Screens Hacked

Smudge Attacks, University of Pennsylvania Aug 2010

Pattern: [215368479]

Apple Patent (2010)
iPhone 5 (?) : "NFC-Fingerprint"

Apple Gearing Up for the Coming NFC- iPhone Revolution

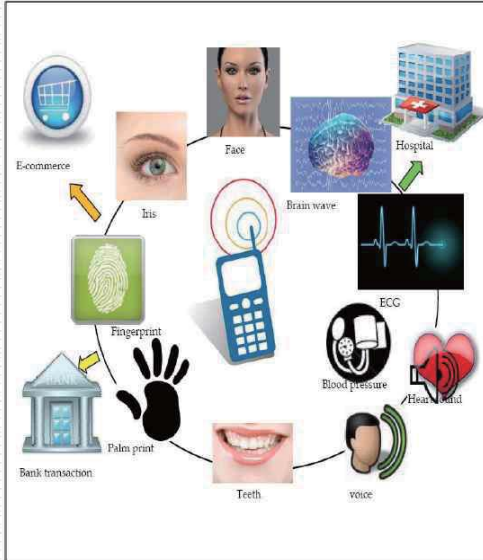
Point-of Purchase System: NFC Interface, Camera & Scanner

How we can enter a PIN, Password, Credit card/ Bank Accounts number?

2016-09-26 8 한국법제연구원 워크숍

I 바이오인식기술 변천사 및 국외동향 - Mobile Biometrics

Concept of mobile Biometrics



Products for mobile Biometrics

Table 14: Company Summary

Company	Country	Biometric modality	Interviewee Name
Asakam, an Equifax Company	USA	Voice	Bront Williams - Chief Technology Officer
Animetrics Inc.	USA	Face	Joel Breen - Vice President
Authentic	USA	Fingerprint	Brent Dietz, Director, Corporate Communications
Authenticate	USA	Voice	John Zurawski, Vice President Sales and Marketing
Bio-Key	USA	Fingerprint	No Interview
Blue Planet Apps, Inc.	USA	Iris, Face, Voice	Jason Draverman - Chief Executive Officer
3M Cogent	USA	Face, Fingerprint, Palm, Iris	No Interview
Dacon (IdentityX)	USA	Face, Palm, Voice	No Interview
LT	USA	Face, Fingerprint, Palm, Iris	No Interview
Mobboot	Spain	Iris, Signature	No Interview
m2SYS	USA	Fingerprint, Finger vein, Palm vein, Iris	John Trader - Communications Specialist
Nuance Communications	USA	Voice	No Interview included for this section. Chuck Buffum interviewed for other sections.
Parsay	Israel	Voice	No Interview
PhoneFactor	USA	Voice	Steve Dispensa - CTO
Precise Biometrics	Sweden	Fingerprint	No Interview
SecurMobile	USA	Voice	No Interview
Transaction Security Inc.	USA	Signature/Sign	Rod Beatson - President and CEO
Voice Commerce Group	UK	Voice	Nick Ogden - Chairman and CEO
VoiceVault	UK/USA	Voice	Nik Stanbridge, Director of Product Marketing

Source: Copyright © Gooda Intelligence 2011

2016-09-26

9

한국법제연구원 워크숍

I 바이오인식기술 변천사 및 국외동향 - Mobile Biometrics

Mobile Biometrics Market (source: 전자신문, '15.2.4)

❖ **2011: 350억원 → 2020: 약36조원 (스마트 모바일기기 시장)**
생체인식, 2020년 개화기 예고

모든 스마트 모바일기기에 탑재 관련 시장 36조원 규모로 확대

오는 2020년까지 스마트폰과 태블릿PC, 웨어러블 기기 등 모든 스마트 모바일 기기에 생체인식 모듈이 탑재되고, 관련 시장 역시 매년 90%의 성장에 연 333억달러(약 36조원) 규모로 커질 것으로 예상된다.

시장조사기업 AMI(Acuity Market Intelligence)는 최근 발표한 '세계 모바일 생체인식 시장 분석 보고서(The Global Biometrics and Mobility Report)'에서 이렇게 전망했다.

금융과 정보기술(IT)의 융합인 '핀테크'에 대한 관심이 뜨거운 가운데 지문인식과 홍채인식 등 생체정보 인식 기술은 공인인증서를 대체할 차세대 보안인증 수단으로 각광받고 있다. 센서인식물 향상, 모듈 소형화 등 부품 기술이 발전하고 차세대 스마트폰과 웨어러블 기기 등에 적용이 점차되면서 관련 시장과 후방 산업계의 성장에 기대된다는 평가다.

핵심 모스트 AMI 대표는 "생체인식은 우리가 깨어 있는 시간 대부분 눈에 들고 있는 스마트 모바일 기기에 가장 적합한 인식모듈"이라며 "오는 2020년에는 모든 스마트 모바일 기기에 생체인식이 기본 탑재될 것"이라고 예상했다.

국내 전자부품 업체도 신규 사업 영역으로 생체인식 분야를 적극 모색하는 추세다. 이미 시장이 준비된 지문인식 분야에서는 관련 전문업체와

터치스크린펜(ETP) 업체가 상용화 노력을 기울이고 있으며, 홍채인식 분야에선 카메라 모듈 업체들이 기존 기술력을 바탕으로 시장개화에 대비하고 있다.

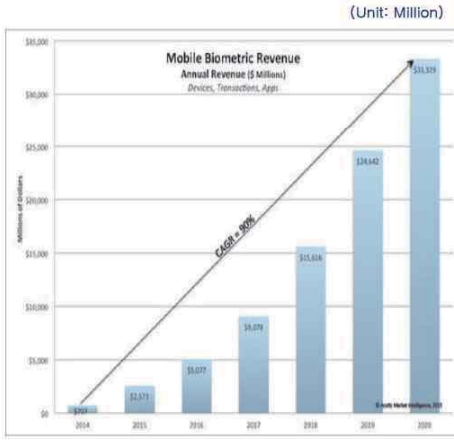
크루셀텍은 지문인식 모듈로 이미 시장에 안착했다. 한 번의 터치로 지문을 읽어내는 에이리어 방식과 지문을 읽어내려 인식하는 스와이프 방식의 두 기술을 모두 보유한 이 회사는 특히 중국 시장을 중심으로 공급을 확대하고 있다. 누적 공급량은 850만대에 달한다. 지난해 화웨이, 오프로 등의 프리미엄급 스마트폰에 적용돼 호평을 받았다.

크루셀텍은 결제서비스 전문업체 다날과 합작해 생체인식 종합 솔루션 기업 바이오팩을 설립하고 지문인식뿐만 아니라 홍채인식과 광학인식 등 다양한 생체정보 기반 인증 솔루션을 준비하고 있다.

TSP 전문업체 트래이스도 지문인식 솔루션 개발에 적극적이다. 최근 모바일 결제 시 지문 인식만으로 결제가 가능한 스마트 결제인증 기술 '비섹(T-SEC)'을 개발했다. 이 기술은 '홍채인'과 같은 별도의 모듈 없이 디스플레이 자체로 지문인식한다. 트래이스는 지난해 산업용상자원부의 지문인식기술 개발 지원사업에 주관사로 선정돼 산업용공공연구망식으로 프로젝트를 진행해왔다.

주요 스마트폰 제품군에 적용이 이뤄진 지문인식과 달리 홍채인식은 이제 막 도입이 검토되는 단계다. 완성률 적용에 앞서 인식 거리와 정확도 등에서 최적화가 진행되고 있다.

빅데이터기자 jespark@etnews.com



〈모바일 생체인식 시장전망(자료 Acuity Market Intelligence)〉

2016-09-26

10

한국법제연구원 워크숍

I 바이오인식기술 발전사 및 국외동향 - ATM Machines

활용국가	적용내용	Bio인증
영국 (홍채)	<ul style="list-style-type: none"> Barclays 은행 (신원도용 피예방지용), '15년~ 인터넷뱅킹 이제거래시 지정맥으로 본인확인서비스 시범운영중 	지정맥 (손가락)
일본 (정맥)	<ul style="list-style-type: none"> 도쿄 미쓰비시 UFJ, 미쓰이 스미토모 등 주요은행권 ATM 거래시 손바닥/손가락 정맥으로 금융사고 예방서비스 실시중 오가키 교리츠 등 일부은행권 무매제 거래를 위해 정맥정보를 은행서버에 저장/관리중 '04년 도입후, '08년 ATM 범죄발생율이 1/3 수준으로 격감 	손바닥 /손가락 정맥
기타 주요국가 (지문)	<ul style="list-style-type: none"> 브라질, Banco do Brazil(지문), Bradesco S.A 은행(정맥) 연금운영비 절감을 위한 본인확인절차 적용중 바이오정보를 IC카드에 저장하여 ATM 거래에 활용하고 있음 인도, State Bank of India(지문) : ATM거래시 적용중 호주/뉴질랜드, 텔레뱅킹에 음성인식 활용중 미국, 중소형 금융기관에서 지문인식 활용중 한국, 대포통장근절을 위한 바이오인식기술 도입 검토중 	지문,홍채, 정맥,음성 인식기술

출처: 금감원 대포통장근절을 위한 공정회(2014.12.7)

I 바이오인식기술 발전사 및 국외동향 - e-Payment (삼성페이)



I 바이오인식기술 변천사 및 국외동향 – Fintech, Healthcare

이데일리 2015년 09월 11일 (수) 종합 1면



위부터 시계 (iAlan) 부터 스마트워치로 변화: 부에나데에서 개최된 iBex에서 한 주 대를 최고경영자(CEO)가 및 웨어러블 기기인 '이클라우'를 소개하고 있다.

**'애플워치' 첫 선... 불꽃은 스마트워치 대전
핀테크·헬스케어 '주도권' 잡아라**

구분	이베인(Urbane) LTE	화웨이 워치	그립
제품 이미지			
제조사	LG전자	화웨이	HTC
화면크기	1.3인치	1.4인치	1.8인치
해상도	320 X 320	400 X 400	32 X 160
Application Processor	스냅드래곤 400	스냅드래곤 400	-
센서	9축(자이로/가속도/자침반), 기압센서, 심박센서, GPS 등	가속도계, 자이로스코프, 센서 및 헬스케어센스 등	조도, 나침반, 자이로, 가속도 등

2016-09-26

13

한국법제연구원 위크숍

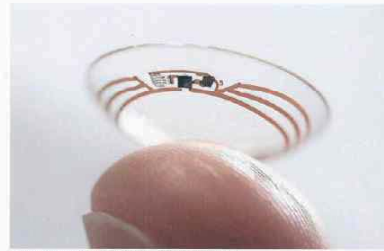
**페이팔... 심장박동, 정맥인식
(월스트리트저널, 2015.4.20)**

THE WALL STREET JOURNAL

20. April 2015, 11:57:24 KST

삼킬 수 있는 패스워드? 페이팔의 차세대 생체인식 기술 화제

Ryland Mitroch



구글의 '웨이브(guon)'를 표지할 수 있는 손맥프린트를 중요 하다.

GOODILLASSOCIATED PRESS

홍차·망막 인식과 지문 인식 같은 생체 인식 시스템은 이제 구식이다?

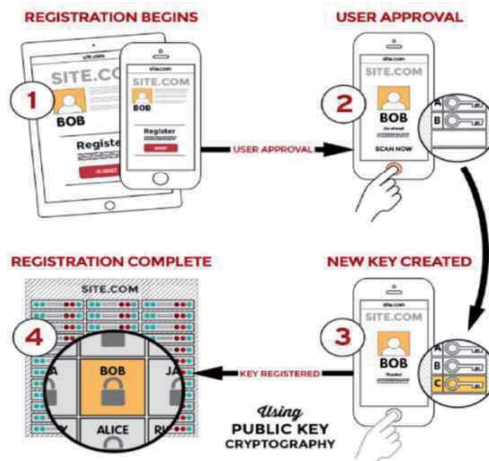
오버와 결재를 비호해 단기간 온라인 거래를 위한 차세대 인식 시스템은 '끼워 넣거나 주입하거나 삼킬 수 있는 기기(embeddable, injectable, and ingestible devices)'라는 것. 웨이브에서 개발자 지원 툴을 제공하고 있는 조니선 프롤립의 주장이다.

최근 그는 미국과 유럽의 다양한 IT 컨퍼런스에서 '월 스트리트저널(All Pass Words)'라는 프레젠테이션을 하기 시작했다. 그는 기술이 현재의 정황으로 증명될 때 기술에 크게 도약할 수 있다고 본다.

그는 생체 인식 방식이 지문 인식과 같은 외부적인 방식에서 심장 박동 인식이나 맥박 인식 같은 내부적인 방식으로 옮겨갈 것이라고 내다봤다.

I 바이오인식기술 변천사 및 국외동향 – FIDO defacto STD

FIDO Alliance



2016-09-26

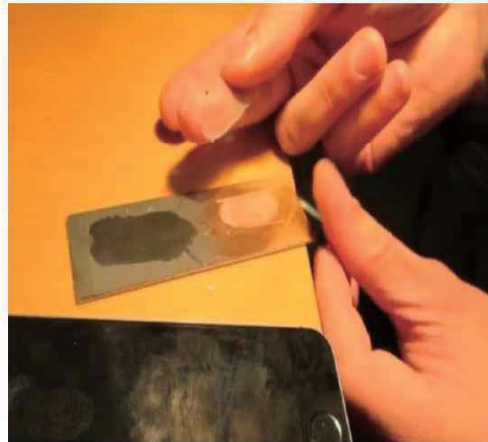
14

한국법제연구원 위크숍

II 바이오인식 보안취약점 및 대책 - Fake Biometrics

Mobile Biometrics based on Smartphone

미국 아이폰5S 모바일 지문인식기능, 가짜손가락에 틀렸다 (보안뉴스, '13.9월)



2016-09-26

15

한국법제연구원 워크숍

II 바이오인식 보안취약점 및 대책 - Fake Biometrics

“증가하는 위조 지문의 위협”

● 위조 지문 제작 방법의 대중화

- 종이/실리콘 위조 지문 제작 방법을 Youtube에 공개
- Google, Youtube에 종이/실리콘/고무찰흙 위조 지문 제작 방법 수십 건 검색
- 일반인도 도장 제작 업체(고무), 의수 제작 업체(실리콘), 인쇄 업체(수지 제판) 통해 고품질 위조 지문을 별다른 제약 없이 제작 가능

● 위조 지문 공격 실제 사례

- http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000743816
- <http://blog.naver.com/tbroadgg?Redirect=Log&logNo=117854858>
- <http://www.bbc.co.uk/news/world-latin-america-21756709>



‘본드막 지문위조’ 사건 흐름도



2016-09-26

16

한국법제연구원 워크숍

II 바이오인식 보안취약점 및 대책 – Threats on biometrics

Biometric System & Attack Points (ITU-T SG17 Q9.Telebiometrics, X.tpp)

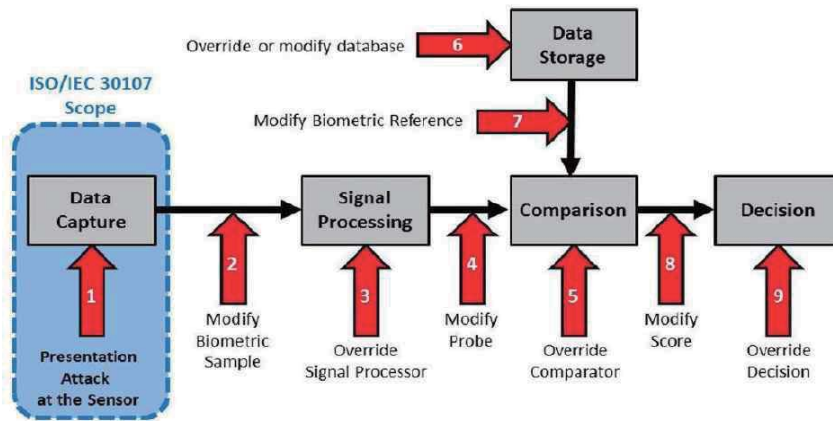


Figure 1 — Examples of points of attack in a biometric system (inspired by [1])

II 바이오인식 보안취약점 및 대책 – PAD(ISO/IEC 30107)

PAD, Biometrics presentation attack detection (ISO/IEC SC37 30107-1,-2,-3)

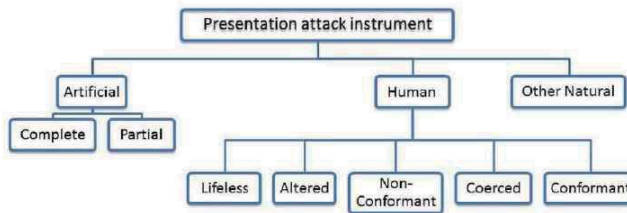


Figure 2 — Types of Presentation Attacks

Table 1 — Examples of Artificial and Human Presentation Attack Instruments

Artificial	Complete	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up
Human	Lifeless	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	facial expression/extreme, tip or side of finger
	Coerced ^{<3>}	unconscious, under duress
	Conformant	zero effort impostor attempt

II 바이오인식 보안취약점 및 대책 - PAD(ISO/IEC 30107-1)

PAD-part1, General Biometric Framework

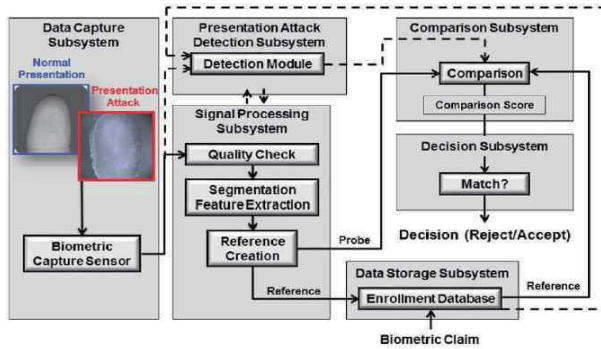


Figure 3 — A general biometric framework with presentation attack detection (other configurations are possible)

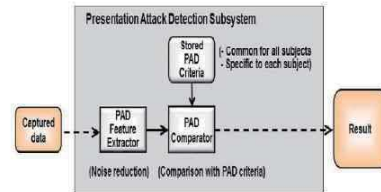


Figure 4 — Components in a general presentation attack detection subsystem

II 바이오인식 보안취약점 및 대책 - PAD(ISO/IEC 30107)

PAD-part2, Data Formats (CD2, developing)

[Scope]

센서에서 발생하는 공격에 대해 PAD 사용과 PAD 결과 제시를 위한 데이터 형식 정의
(PAD output & PAD input)

XML schema와 binary format 포괄 정의

[Reference]

ISO 8601:2004, Data elements and interchange formats – Information interchange – Representation of dates and times

ISO/IEC 19785-1:-, Information technology – Common Biometric Exchange Formats Framework –
Part 1: Data element specification

ISO/IEC 19794-1:2011, Information technology – Biometric data interchange formats – Part 1: Framework

ISO/IEC 30107-1:-, Information technology – Presentation attack detection – Part 1: Framework

II 바이오인식 보안취약점 및 대책 - PAD(ISO/IEC 30107)

PAD-part3, Testing and Reporting (CD1, developing)

[Scope]

PAD 테스트 방법 정의

평가 결과와 보고서 출력 정의, Presentation attacks 분류

[Reference]

ISO/IEC 2382-37, Information technology – Vocabulary – Part 37: Biometrics

ISO/IEC 18045, Information technology – Security techniques – Methodology for IT security evaluation

ISO/IEC 19792:2009, Information technology – Security techniques – Security evaluation of biometrics ISO/IEC 19794-1:2011, Information technology – Biometric data interchange formats – Part 1: Framework

ISO/IEC 19795-1:2006, Information technology – Biometric performance testing and reporting – Part 1: Principles and framework




II 바이오인식 보안취약점 및 대책 - PAD(ISO/IEC 30107)

PAD-part3, Testing and Reporting (CD1, developing)

PAD 테스트 특성

일반적인 바이오인식 성능평가와는 차이점 존재

- 공격 재료의 다양성
- 결과 분석의 차이
- 협조적인 테스트
- 자동화 테스트
- 테스트 DB 품질과 성능의 관계

Artefact species	Description	Illustration
Silicon finger artefact	Matte or glossy	
Laser print finger artefact	Ordinary 2D print out	
Gelatin finger artefact	Half-transparent gelatin with glycerin	

III 바이오인식기술 관련 KISA 대응연황 - 추진연혁



2016-09-26

23

한국법제연구원 워크숍

III 바이오인식기술 관련 KISA 대응연황 - PAD 시험(2007년)

■ KISA 위조지문 BMT 시험기준 (행자부 무인민원발급기, 2007.7월)

- 위조지문 종류 : 종이, 필름, 실리콘, 젤라틴, 고무
- 위조지문 BMT 시험방법
 - 제작된 위조지문을 지문인식 센서를 통해 이미지화
 - 실제지문(10명, 4대 발급기별 3회 스캔/발급 확인시험)
 - 4종 위조지문(흑백종이, OHP 필름, 실리콘, 젤라틴 제작) 각센서당 3회 모조지문 감별 확인
 - 피시험자(지문제공자, 연령 20~40대 남녀 총12명), 참관자(언론기자, 행사부 지자체 담당자)
- 검증 시나리오

시나리오 (Scenario)	등록(Enrollment)	인증(Authentication)
실제 - 위조	실제 지문	위조 지문
위조 - 실제	위조 지문	실제 지문
위조 - 위조	위조 지문	위조 지문

- 위조지문 비공개 BMT 시험결과
 - 실제지문의 경우, C社 지문인식기 성능저하(인증시도 7회) 확인
 - 종이모조지문(A社 스캔오류), OHP필름(4개社 탐지), 실리콘(4개社 탐지), 젤라틴(3개社 실패)
 - 2008년이후 1,564대 무인민원발급기에 위조지문 판별가능한 지문인식기로 전면 대체됨

2016-09-26

24

한국법제연구원 워크숍

III 바이오인식기술 관련 KISA 대응연향 - 국내표준화 활동

The screenshot shows the KISA website interface with a search filter for '생체인식기술' (Biometric Recognition Technology). A table lists various standards with columns for No., 표준번호 (Standard No.), 표준명 (Standard Name), and 제/개정일 (Issue/Revision Date).

No.	표준번호	표준명	제/개정일
21	TTAK-KO-12.0195	바이오 보안 로그인 API	2011-06-29
20	TTAK-KO-12.0190	바이오 인의 정보 및 개인 식별 정보 데이터베이스의 분리 출항 방법	2010-12-23
19	TTAK-KO-12.0188	얼굴 검출을 이용한 CCTV 영상 정보 프라이버시 보호를 위한 보안 요구사항	2010-12-23
18	TTAK-KO-12.0182	[개정] 바이오인식 결과	2010-12-23
17	TTAK-KO-12.0180	얼굴 인식 시스템 시리얼노가변 성능 시험 방법	2010-12-23
16	TTAR-12.0008	영상 캡처 시스템에서의 적외선 및 인공광의 분석 (기술보고서)	2010-11-24
15	TTAR-12.0008	부조지문 압지 기술 (기술보고서)	2010-11-24
14	TTAK-KO-12.0177	현금자동입출금기(계좌의 시열적 영상) 생성 지원 방법	2008-12-22
13	TTAEJT-11.0084	통신망에서의 바이오인식 시스템 인증 체계 수립	2009-12-22
12	TTAK-KO-12.0166	인식률 향상 및 바이오 인식 정보 보호를 위한 제로 및 전송 보강	2009-12-22
11	TTAK-KO-12.0165	자문인식 알고리즘 성능 시험 지침	2009-12-22
10	TTAK-KO-12.0164	얼굴 검출 기술 시스템의 보안 요구사항	2009-12-22
9	TTAR-12.0004	자문인식 시스템의 인장성 확보를 위한 자문인식기의 취약점 분석	2009-11-24
8	TTAK-KO-12.0097	스카프카드 기반의 지문채취용 방법론	2008-12-19
7	TTAK-KO-12.0096	바이오 인식 정보에 기반한 전자서명 생성 지원 방법	2008-12-19
6	TTAK-KO-12.0095	얼굴 검출 기술의 성능 평가 방법	2008-12-19
5	TTAS-KO-12.0039	얼굴 검출 기술의 성능 평가 방법	2007-06-22
4	TTAS-KO-12.0047	인장성 확보를 위한 자문인식기의 취약점 분석	2008-12-27
3	TTAS-KO-12.0046	자문인식 결과 품질 분류 방법	2008-12-27
2	TTAS-O1-10.0039	BioAPI 표준화할 것 시험안 및 별지(K-CIS)	2008-12-25

2016-09-26
25
한국법제연구원 워크숍

III 바이오인식기술 관련 KISA 대응연향 - 국제표준화 활동

The screenshot shows the KISA website interface with a search filter for '생체인식기술' (Biometric Recognition Technology). A table lists various international standards with columns for 표준화 상태 (Standardization Status), 국제표준 국제번호 (International Standard No.), 표준명 (Standard Name), 에디터 (Editor), and 표준 내용 (Standard Content).

표준화 상태	국제표준 국제번호	표준명	에디터 (국가/소속)	표준 내용
ISO/IEC (2011)	ISO/IEC SC27 24746	Biometric Information Protection	전영민(한국표준연구원)	생체정보 보호기술 표준
DIS (2016.10)	ISO/IEC SC27 17922	Biometric authentication framework - Biometric hardware security module	전영민(한국표준연구원)	생체인식기술(BIOS)와 하드웨어 보안 모듈
TR (2007)	ISO/IEC SC37 24722	Multi-Modal Biometrics	송경(ETRI)	다중생체인식기술 연구보고서(TR)
ISO/IEC (2007)	ISO/IEC SC37 24709-1	Conformance Test for Bio API: part 1 - Test method and procedures	권세성(KISA)	BioAPI 적화성 시험기술 표준
ISO/IEC (2007)	ISO/IEC SC37 19794-9	Biometric data interchange format - Part 9: Vascular image data	최진수 (테크스피어)	생체인식 데이터 교환규격
ISO/IEC (2014)	ISO/IEC SC37 19794-14	Biometric data interchange format - Part 14: DNA data	김현수(국립수사연구원)	DNA 데이터 교환규격
TR (2014)	ISO/IEC SC37 29198	Characterization and measurement of difficulty for fingerprint databases for evaluation technology	권진원(한국표준연구원)	생체정보 활용 기술의 난이도 측정기술 연구보고서(TR)
PDTR3 (2016.6)	ISO/IEC SC37 30108	Use of Biometrics for Personalization and Authentication	Fred Preston (영국), 권세성(KISA)	2차원 생체인식 사용자 기술 연구보고서(TR)
CD2 (2016.6)	ISO/IEC SC37 24709-1R1	Conformance Test for Bio API: part 1 - Test method and procedures(revision)	권세성(KISA)	BioAPI 적화성 시험기술 표준(개정)
DIS (2016.6)	ISO/IEC SC27 19794-15	Biometric data interchange format - Part 15: Palm cross image data	전영민(한국표준연구원)	손가락 데이터 교환규격
CD (2016.6)	ISO/IEC SC37 30137-2	Use of biometrics in video surveillance systems - Part 2: Performance testing and reporting	권진원(한국표준연구원)	영상 CCTV 활용기술-2차원 영상 평가(TR)
NP (2016.6)	ISO/IEC SC37 30106-AMD1	OO-BioAPI-Part1:Architecture- Amendment 1: Additional spec and Conformance Statements	권세성(KISA), Raul Sanchez(스페인)	국제적용형 BioAPI 적화성 시험기술

2016-09-26
26
한국법제연구원 워크숍

III 바이오인식기술 관련 KISA 대응연방 - 국제표준화 활동

ITU-T SG17/Q9 한국 추진현황(텔레바이오인식분야)

표준화 상태	국제표준 과제번호	표준명	에디터 (국가)	표준 내용
ITU-T X.1086 (2008)	X.tpp-1 X.1086	Telebiometrics Protection Procedures Part1(A guideline of technical and managerial countermeasures for biometric data security)	김재성(KISA)	텔레바이오인식정보보호기술1관-기술적/관리적 보안대책
ITU-T X.1088 (2008)	X.tdk X.1088	Telebiometrics Digital Key: A framework for biometric digital key generation and protection	이영우(관신대) 김재성(KISA)	텔레바이오인식 디지털 키 생성 및 보호기술
ITU-T X.1089 (2008)	X.tsm X.1089	Telebiometrics System Mechanism - Part1: General biometric authentication protocol and profile for telecommunication systems	Isobe(이디지) 신용녀(KISA)	텔레바이오인식 인종기술
ITU-T X.1092 (2013)	X.tif X.1089	Integrated framework for telebiometric data protection in e-Health and worldwide telemedicine	김재성(KISA)	텔레바이오인식기반 원격의료서비스
6th WD (2016.9)	X.tam X.1092	A guideline to technical and operational countermeasures for telebiometric applications using mobile devices"	김재성(KISA) 신용녀(KISA)	모바일기기 텔레바이오인식 응용기술 (FIDO로써 표준?)
DIS (2016.9)	X.bham X.1086	Telebiometric authentication framework using biometric hardware security module	김재성(KISA) 권영근(중북대)	공인인증서(X.600)와 텔레바이오인식 응용기술

2016-09-26

27

한국법제연구원 워크숍

III 바이오인식기술 관련 KISA 대응연방 - 국제협력활동

ABC2012 ('12.11, 제주)



BBC2013 ('13.9, 미국 댄퍼)



MOU with EAB ('13.2, 브뤼셀)



ABC2014 ('14.12, 부어), ISO/IEC SC37 ('15.1, 스페인)



2016-09-26

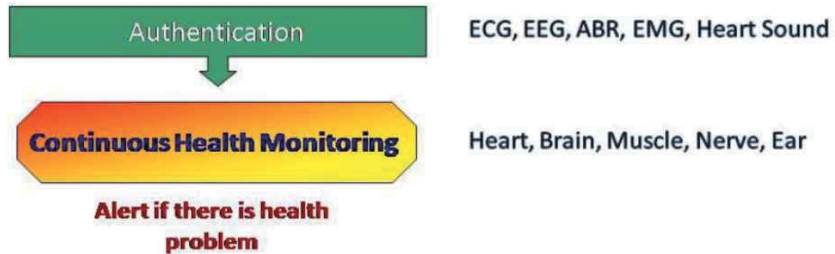
28

한국법제연구원 워크숍

IV Medical Biometrics 기술현황 및 전망, Bio-signals

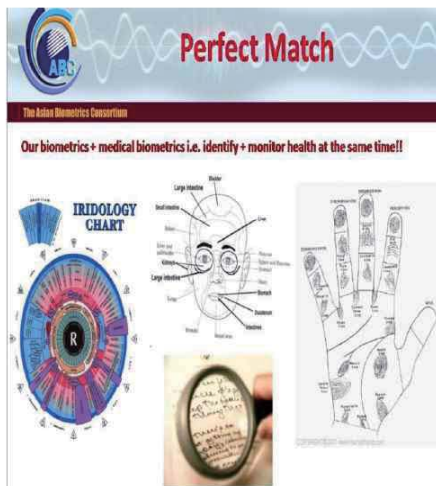
▶ **MEDICAL(COGNITIVE WITHIN BEHAVIORAL BIOMETRICS) BIOMETRICS = 2 IN 1**

- **Doing 'medical biometrics' will waste processing source and time**
 - Biometrics authentication processing
 - Medical biometrics processing
- **Better way to do authentication and health monitoring at the same time is using bio-signals**
 - Same features are used for both purposes
 - Suitable for daily/weekly application e.g. physical access to office



IV Medical Biometrics 기술현황 및 전망, Bio-signals

ABC2011, Malaysia 공과대학



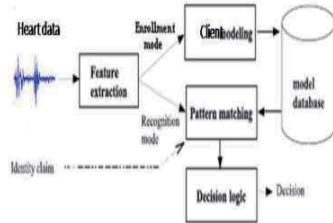
TYPES OF BIO-SIGNAL



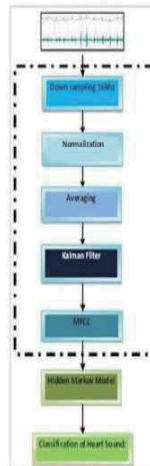
Others e.g. Electrooculography (EOG) – measurement of the resting potential of the retina.

IV Medical Biometrics 기술현황 및 전망, Bio-signal Authentications

▶ HEART SOUND AS MEDICAL BIOMETRICS



- We are only concentrate on medical application with our database
- Now we are moving into *biomedical biometrics*, so we just got preliminary results
- 20 clients vs more than 20 impostors

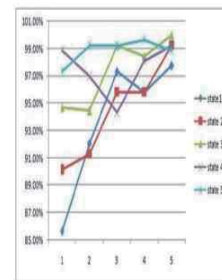


- Welch-Allyn meditron electronic stethoscope
- Location : V1 (aortic)
- 5 normal vs. 5 abnormal
- Change number of HMM states and mixtures



state/mix	1	2	3	4	5
1	85.61%	90.15%	94.70%	98.06%	97.33%
2	92.05%	91.29%	94.45%	96.57%	99.34%
4	97.33%	95.83%	95.24%	94.32%	99.34%
8	95.83%	95.83%	90.48%	98.11%	99.62%
16	97.73%	99.24%	100%	99.24%	98.66%

Average 93.73% 94.47% 97.37% 97.50% 98.86%



- Best combination : 3 state 16 mixtures

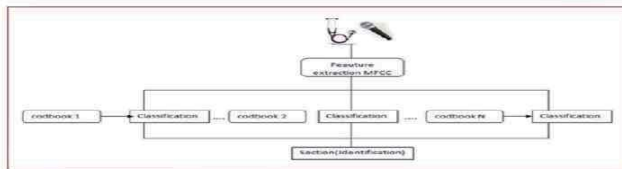
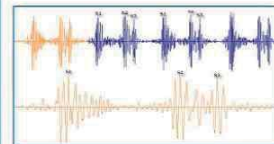
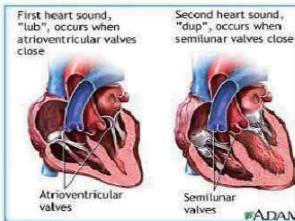
2016-09-26

31

한국법제연구원 워크숍

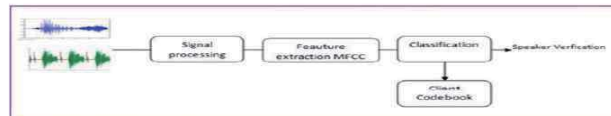
IV Medical Biometrics 기술현황 및 전망, Bio-signal Authentications

▶ HEART AND SPEECH SOUNDS AS MEDICAL BIOMETRICS



Identification
Are you really one of us?
1 : N authentication

Verification
Seriously, you are him/her?
1 : 1 authentication



2016-09-26

32

한국법제연구원 워크숍



Neuroelectronics

- ❖ Mobile, comfortable, precise and robust wireless EEG
- ❖ Medical grade EEG devices with 8, 20 and 32 channels
- ❖ 24 bits resolution, 500Hz



- ENOBIO 8
- 8 EEG channels
- 3,995 €

<http://www.neuroelectronics.com/>



- ENOBIO 20
- 20 EEG channels
- 12,495 €



- ENOBIO 32
- 32 EEG channels
- 19,995 €

2016-09-26

33

한국법제연구원 워크숍



NeuroSky

- ❖ MindWave Mobile
- ❖ Affordable research-grade EEG headset
- ❖ 1 EEG channel, 512Hz
- ❖ \$99.99 USD



2016-09-26

34

한국법제연구원 워크숍

IV Medical Biometrics 기술현황 및 전망, Wearable Devices for ECG

Nymi (BioNym)

- ❖ 유일한 ECG 기반의 개인인증 웨어러블 디바이스
- ❖ HeartID: Nymi's patented biometric authentication technology
- ❖ Wristband 타입
- ❖ Raw ECG Stream 취득 가능
- ❖ \$149 USD



2016-09-26

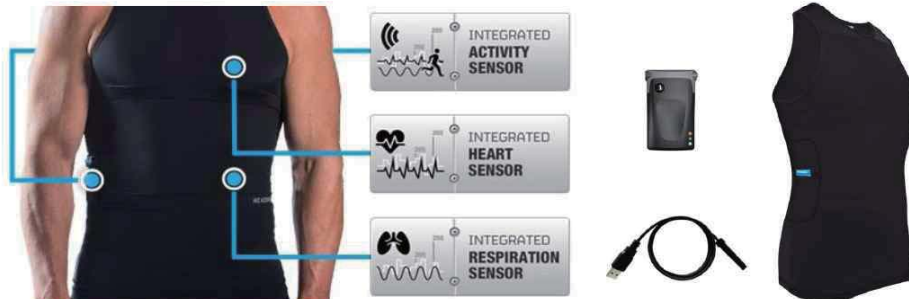
35

한국법제연구원 워크숍

IV Medical Biometrics 기술현황 및 전망, Wearable Devices for ECG

HexoSkin (Carre Technologies, Inc)

- ❖ Biometric shirt
- ❖ Heart Rate, Heart Rate Variability, Breathing Rate, Breathing Volume, Activity, Sleep
- ❖ \$399 USD



<http://www.carretechnologies.com/>
<http://www.hexoskin.com/>

2016-09-26

36

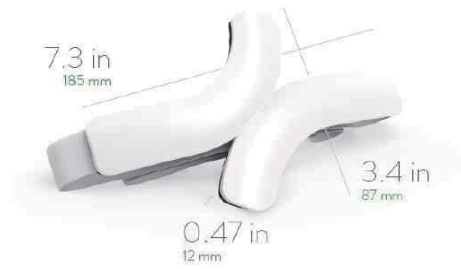
한국법제연구원 워크숍

IV

Medical Biometrics 기술현황 및 전망, Wearable Devices for ECG

QardioCare (Qardio, Inc)

- ❖ Medical-grade wearable ECG monitor (3 channels)
- ❖ 출시 전



2016-09-26

37

한국법제연구원 워크숍

IV

Medical Biometrics 기술현황 및 전망, Wearable Devices for PPG

Heart Rate Sensor

- ❖ 피트니스 목적의 Wristband / Smart Watch에 탑재
- ❖ 대부분의 장치가 광학(PPG: 광용적맥파) 센서를 사용
- ❖ 소모전류 및 운동 중 센싱 신호 정확도 개선하기 위해 바이오 임피던스 센서 사용하는 장치도 최근 출시

Optical Heart Rate Sensor
PPG (Photoplethysmography)

vs.

Bio-impedance Sensor



2016-09-26

38

한국법제연구원 워크숍

IV Medical Biometrics 기술현황 및 전망, Wearable Devices for PPG

Wearable Devices



- Apple Watch
- PPG Sensor
- \$349.00 USD +



- fitbit Charge HR
- PPG Sensor
- \$149.95 USD



- Samsung Gear S
- PPG Sensor
- ₩327,000



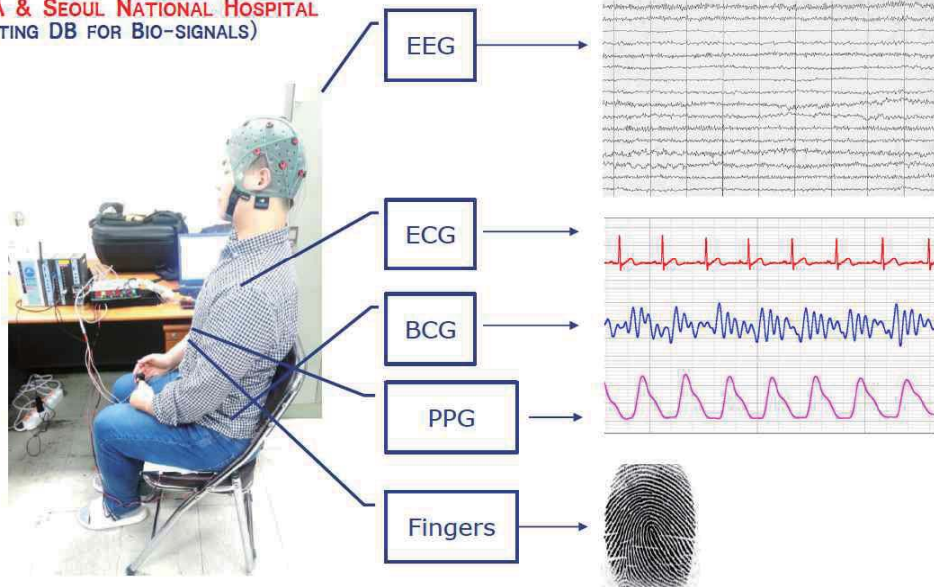
- Jawbone UP3
- Bio-impedance
- \$179.99 USD



- LG Watch Urbane
- PPG Sensor
- ₩587,600

V KISA 생체신호 인증기술 개발현황 및 향후계획, KISA 국제공동연구

▶ KISA & SEOUL NATIONAL HOSPITAL
(TESTING DB FOR BIO-SIGNALS)



✓ KISA 생체신호 인증기술 개발현황 및 향후계획, KISA 국제공동연구

- ❖ **Test Results for ECG Authentication (81.67%)**
 - Imposter mode, Euclidian distance 기반 threshold
 - CRR = 81.67%
 - EER = 18.32%
 - Threshold level
 - empirically decided
- ❖ **Summary of Testing Results for Bio-signals**
 - **Identity Tests for Bio-signals**
 - ECG (99.5%) > EEG(eye-close) (96.8%) > EEG(eye-open) (93.2%) > PPG (89.8%) > BCG (73.6%)
 - **Authentication Accuracy Tests for Bio-signals**
 - ECG (84.34%) > EEG (eye-close) (78.0%)
 - **ECG has best identity and authentication accuracy among bio-signals**
 - **Multi-modal bio-signals give raise to more higher authentication accuracy degree.**

2016-09-26 41 한국법제연구원 워크숍

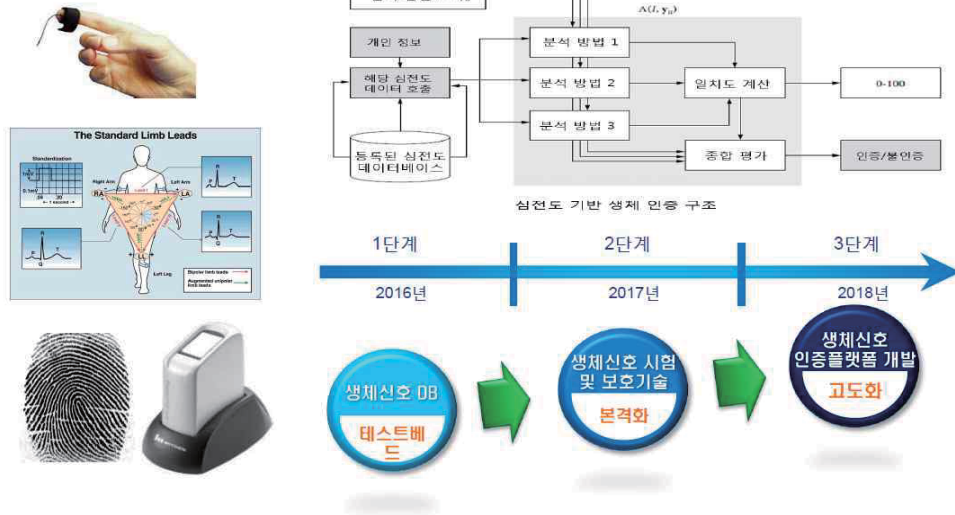
✓ KISA 생체신호 인증기술 개발현황 및 향후계획, KISA 국제공동연구

▶ **DEVELOPMENT OF TELEBIOMETRIC AUTHENTICATION FOR ECG & FINGERPRINT**
 (2016.7~2018.12, 14억원, 주관기관: KISA, 참여기관: 스페인-마드리드, 미국-TELEBIOMETRICS)

2016-09-26 42 한국법제연구원 워크숍

✓ KISA 생체신호 인증기술 개발현황 및 향후계획, KISA 국제공동연구

▶ MILESTONES



✓ KISA 생체신호 인증기술 개발현황 및 향후계획, KBID와 공동대응

❖ **바이오정보 보호기술 대응전략**

- 바이오정보보호 가이드라인 중용시험 인증서비스 추진검토중
- 핀테크분야에서의 ISO/IEC PAD 준용시험 인증서비스 추진검토중
- 바이오정보 보호를 위한 기술적/관리적 대책 TTA 단체표준 → KS 국가표준화 추진
- 범정부차원의 바이오인식기술 활용 및 보호에 관한 법제화 연구 필요성 검토

❖ **핀테크·헬스케어·스마트카 등 차세대 비대면 인증기술 개발전략**

- 스페인, 미국 등 주요선진국과 심전도(심박수)·지문 등 다중 생체신호 인증기술 국제공동연구 추진중
- ITU-T SG17 Q9(Telebiometrics) 국제표준화(X.tab) 추진중
- 워변조에 강인한 비대면 인증기술로 차세대 바이오인식기술로 시장창출 및 관련산업(핀테크, 헬스케어, 스마트카 등) 활성화 촉진

The central graphic features a stylized globe with yellow and blue continents. On top of the globe, several 3D figures of people in business attire are shown in various poses, some holding up buildings. The globe is surrounded by logos for the Asian Biometric Consortium (ABC), KISA (Korea Internet & Security Agency), and the European Association for Biometrics (EAB). The ABC logo is on the left, KISA is in the center, and EAB is on the right. The KISA logo includes the text 'KISA 한국인터넷진흥원' and 'KISA 바이오인식협의회'.

미국
the biometric CONSORTIUM

유럽
European Association for Biometrics
eab
Human Identity in Europe

- KISA 보안기술확산팀 연구위원(공학박사)
- TTA PG505(바이오인식) 국내 표준화위원장, 미래부 국립전파연구원 KS 국가표준 심의위원
- 아시아바이오인식협의회(ABC) 회장, ISO/IEC SC37 & ITU-T SG17/Q9 국제표준전문가(에디터)
- jskim@kisa.or.kr, +82-2-405-5367

2016-09-26 한국법제연구원 워크숍

생체인식 정보의 처리에 관한 개인정보 보호법제의 현황과 개선방향

이 은 우
(법무법인 지향 변호사 · 정보인권연구소 이사)

1. 용어의 문제

가. 무엇을 규율하려는 것인가?

- 신체적, 행동적 특징에 관한 정보 vs 고유하게 식별하는 정보
- 신체적, 행동적 특징에 관한 정보를 기계가 가독할 수 있도록 처리한 것,

나. 현상을 왜곡하는 ‘바이오 정보’ 용어라는 용어는
폐기해야 한다.

정통망법 시행령

④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

<개정 2014.11.28.>

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호, 계좌정보 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장

개인정보의 기술적·관리적 보호조치 기준(방통위)/ 개인정보의 안전성 확보조치 기준(행자부)

“바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

제 7 조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

바이오 정보보호 가이드라인 (2007. 9)

- 1. “바이오정보”라 함은 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다.

다. 생체정보보다는 ‘생체인식 정보’라는 것이 정확하다

(1) 현재의 법령상 ‘생체정보’

전자금융거래법

10. “접근매체”라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.

가. 전자식 카드 및 이에 준하는 전자적 정보

나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조제7호의 인증서

- 다. 금융회사 또는 전자금융업자에 등록된 이용자번호
- 라. 이용자의 생체정보
- 마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

국방생체정보보호 지침¹⁾

“생체정보”라 함은 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다.
② “생체인식시스템”이라 함은 지문인식, 홍채인식, CCTV 등 생체정보를 이용하여 개인을 식별하는 정보시스템을 말한다.

나라장터 생체인식(바이오)보안기기 제품 지정 및 관리 규정

“생체정보”란 지문·얼굴·홍채·정맥 등 개인을 식별할 수 있는 신체적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다.

(2) 생체정보보다는 생체인식 정보가 바람직

- 개인정보보호법제에서 보호하고자 하는 대상은 ‘생체정보’ 그 자체가 아니라, ‘생체인식정보’이기 때문임.
- 개인을 식별하기 위하여 처리하는 것을 규율하려는 것임.

1) 생체인식시스템 운영하는 국방부/각군/기관이 개인 식별을 위해 이용하는 생체정보를 보호하기 위하여 준수하여야 할 사항을 정함으로써 생체정보의 안전한 이용 환경을 조성함을 목적으로 함.

2. 생체인식 정보에 대한 우리나라의 현재의 법제 상태

가. 생체인식정보는 개인정보에 해당하므로 개인정보 보호법이 적용됨(일반적용)

- 개인정보 : “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
- 수집
- 제3자 제공

나. 생체인식 정보, 바이오 정보 해당 여부

- 사진, 음성 녹음, 영상(CCTV) 모두 정통방법의 바이오 정보 해당함.

다. 정통방법 시행령과 방통위 고시, 행자부 고시에 의해서 암호화 저장하여야 함.

- 바이오 정보 : 지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보
- 암호화 저장 : 제7조(개인정보의 암호화) ① 개인정보처리자는 고유 식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
- 이 규정에 의하면 ‘사진’, ‘노래’도 암호화해야 함.

라. 그러나 영상처리장치는?

제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.(이하 생략)

마. 생체인식정보는 민감정보에 해당하는가?

- 민감정보란? : 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보

제18조(민감정보의 범위) 법 제23조 각 호 외의 부분 본문에서 “대통령령으로 정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

- 민감정보에 대한 규율
- 별도 동의를 받아야 함
- 예외 규정 적용 없음.

제23조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

- 민감정보로 보지 않음. 지문도.
- 단, 유전 정보는 해당할 수 있음.

3. 바이오정보보호 가이드라인의 평가와 효력

가. 정의 규정 애매함

- 개인식별에 이용하는 바이오정보 및 바이오인식시스템에 대해 적용한다.
- “바이오정보”라 함은 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별 할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하

며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다.

- “바이오인식시스템”이라 함은 바이오정보를 이용하여 개인을 식별하는 정보시스템을 말한다.
- 바이오인식시스템의 정의가 애매함.
- 바이오인식시스템 운영자

나. 적용범위

- 현 가이드라인은 바이오인식시스템 운영자를 대상으로 함
- 정보시스템의 정의 모호함(“바이오인식시스템”은 원본정보의 수집, 특징정보 추출·저장·전송 및 식별 등 일련의 과정을 수행하는 정보시스템이다.)
- “바이오정보를 이용하여 개인을 식별하는 정보시스템” vs “생체인식 정보를 개인을 식별하기 위하여 처리하는 경우”
- 전자보다는 후자가 좀 더 정확할 것임.

다. 획일적 - 위험기반 접근이 아님

- 동의 예외 규정이 적용되는지 애매함.
- 다른 점
 - 14세 → 18세 (법정대리인 동의),
 - 운영자는 수집한 원본정보를 보관하는 경우에는 성명·주민등록번호·주소 등 제공자를 알 수 있는 정보와 별도로 분리하여야 한다.
- 나머지는 정통방법과 동일함.

라. 개인정보보호와 관련한 원칙을 구체화할 필요가 있음

- 우리나라 법제에서는 원칙의 규범적 효력이 인정되지 않음.
- 이익형량이 의미가 없음.
- 반면유럽연합은 이익형량을 해야 한다는 점을 명시함.

마. 법률적 효력이 없음.

- 가이드라인에 불과

4. 생체인식정보에 대한 특별한 보호가 필요한가?

가. 생체인식정보 특징과 보호필요성 : universal, unique, permanent, collectability, performance, acceptability, circumvention

나. 신체적, 행동적 특징으로 특정 개인을 고유하게 식별할 수 있다는 위험성

- 식별성의 수준
- 익명성의 침해

다. 불변성

라. 은밀한 수집 가능성

마. 오류 가능성

바. 위험 평가

5. 유럽연합의 경우
- GDPR의 입법으로 변경되는 것

가. GDPR 제정

나. 내용 - 개인식별 위한 생체인식정보를 특별한 범주의 개인정보로 보호함.

(1) 정의 규정에서 유전자 정보, 건강에 관한 정보, 생체인식 정보를 정의함

(13) ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(2) 생체인식정보를 개인 고유하게 식별하기 위해 처리하는 경우는 민감정보(특별한 범주의 정보)의 처리로 보고 특별 보호

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(3) 처리 가능한 경우

2. Paragraph 1 shall not apply if one of the following applies:

- (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of

the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

6. 어떻게 보호할 것인가?

가. 현재의 법령상 문제점

(1) 정의 부적절

(2) 정통방법의 암호화 부적절

- 현재의 규정은 사진도 암호화

(3) 가이드라인 부적절

나. 생체인식정보에 대한 정의를 둘 필요 있음

- 현재의 바이오정보의 정의를 수정할 필요
- “지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체

적 또는 행동적 특징에 관한 정보(로서 그로부터 가공되거나 생성된 정보)” → 생리적 특징 포함. 고유한 식별성 포함 시켜야 함.

‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

다. 보호의 범위

- 모든 생체인식정보가 아니라, 개인식별 위한 경우만

라. 보호의 방법 : 개인식별 위한 목적의 처리시에는
민감정보에 준하는 수준으로(현재는 예외규정이
적용되지 않아서 약간 완화할 필요)

- 개인식별을 위한 처리시에는 ‘민감정보’의 수준으로 보호할 필요
- **processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,**

마. 보호수준의 검토

- (1) 목적 제한
- (2) 최소수집
- (3) 비례성
- (4) 적합성
- (5) 투명성

(6) 안전장치 필요성.

바. 입법의 방법

- (1) 입법은 명료하게
- (2) 이익형량 규정을 구체화할 필요가 있음.
- (3) 필요한 것과 원칙으로 남겨둘 것의 구별

〈 별표 〉

바이오정보 및 바이오인식시스템 기술적·관리적 보호 조치사항

구분		세부내용
〈 공통보호조치 〉		
관 리 적 보 호 조 치	기술적 보 호 조 치	<ul style="list-style-type: none"> ● 바이오정보를 수집·보관·전송·파기시 침해방지를 위한 보호조치를 취한다. <ul style="list-style-type: none"> - 바이오정보의 수집·보관·전송시 암호화 메커니즘 사용 - 바이오정보 파기 시 겹쳐쓰기(Overwrite), 물리적 파괴(Destroy) 등 복원할 수 없는 방법으로 파기
	인적 관 리	<ul style="list-style-type: none"> ● 바이오정보의 안전한 취급을 위한 내부규정을 마련하여 제공자가 쉽게 볼 수 있도록 조치한다. <ul style="list-style-type: none"> - 바이오정보관리책임자의 권한과 책임을 명확히 규정 - 가이드라인의 이행을 위한 세부적인 절차 및 지침을 규정 ● 바이오정보관리책임자 및 취급자를 대상으로 가이드라인 및 내부규정 등을 정기적으로 교육·훈련
	접 근 통 제	<ul style="list-style-type: none"> ● 바이오정보 및 바이오인식시스템에 대한 접근을 통제한다. <ul style="list-style-type: none"> - 접근통제 절차 마련 및 시행 - 바이오정보의 수집·보관·전송·파기에 대한 권한의 차등 부여 - 인사이동, 퇴직 등의 변동사항 발생시 접근권한을 즉시 변경 - 저장매체 등의 반출·입 대상 작성
	운 영 관 리	<ul style="list-style-type: none"> ● 바이오정보 및 바이오인식시스템 침해사고 발생시 조치 및 보고 등에 대한 체계적인 대응지침을 마련한다.
침해사고 조치		<ul style="list-style-type: none"> ● 바이오정보 및 바이오인식시스템에 침해사고가 발생한 경우 대응지침에 따라 신속한 대응조치를 취한다.
〈 특별보호조치 〉		
구분		세부내용
원 본 정 보 보 관 시		<ul style="list-style-type: none"> ● 바이오정보 및 바이오인식시스템이 설치된 장소를 보호구역으로 설정하고, 보호구역에 대한 보안대책을 마련한다. <ul style="list-style-type: none"> - CCTV 등 모니터링 시스템 설치 - 시건장치 등 물리적 접근제어를 위한 시스템 설치 ● 인가받지 않은 사용자의 보호구역 내 출입을 통제한다. <ul style="list-style-type: none"> - 출입허가 인원과 그 외의 방문자가 출입하기 위한 절차 마련 및 시행
외 부 망 연 결 시		<ul style="list-style-type: none"> ● 바이오인식시스템의 전자적 침해를 방지하기 위한 조치를 취한다. <ul style="list-style-type: none"> - 침입차단시스템, 침입탐지시스템 등 정보보호시스템의 설치 - 웜, 바이러스 등 악성프로그램을 점검·치료할 수 있는 백신프로그램의 설치 - 바이오인식시스템의 취약성을 보완하는 보안 패치 프로그램의 설치

토 론 문

생체정보의 현황(패러다임 변화) 및 입법 전략에 대한 고찰

방 동 회
(부산대학교 법전문 교수)

I. 생체정보의 사용 패러다임 변화

- 공공기관에서 사용 ---> 민간 전역에 확대
- 집단적 · 대규모 사용 ---> 개인화된 사용
- 공공기관의 통제 ---> 사적 통제영역 으로 확대 변화
- 생체정보의 공적 사용 등 ---> 생체정보 자체가 매우 중요한 재산적 가치와 연결되는 상황
- 생체정보의 침해 유형 내지 유출 형태 다변화
- 생체정보의 왜곡 사용 빈도 및 가능성 매우 증가
- 생체정보의 사용에 있어서 이해관계자 확대

II. 생체정보에 관한 현행 법제의 대응 상황

- 생체정보의 개념, 정의, 범위 불명확
 - 법률마다 개념 분산, 명확성 부재
- 생체정보의 유출 침해에 대한 일반적 규율
 - 개인정보처리자, 정보통신서비스제공자의 행위규제)로 그치고 있는 상황
 - 특히, 생체정보의 특성을 고려하여 보호의 방식이 정해진 것이 아니라 일반적인 개인정보의 규율방식에 근거하여 규율하고 있는 상황
- 생체정보의 오남용으로 인한 제2차의 신체적 재산적 피해에 대해서는 거의 무방비 상황

- 법경제학적 측면에서 실효성 있는 제재수단 매우 미흡
- 생체정보의 이해관계자 규율에 있어 특히 민간부분에 있어서는 “동의”만 있으면 수집 활용이 가능한 상황이어서 그 “동의”가 대등한 상황에서 이뤄질 수 있는가?가 의심스러운 상황
- 즉, 강요된 “동의”를 받을 수 있는 상황에 놓이게 됨으로써 서비스제공자에 대한 최소한의 규제 필요성이 증대

Ⅲ. 외국법제에 대한 평가 및 우리 법제에의 시사점

- 유럽을 제외한 일본, 미국, 프랑스 법제는 생체정보에 특화된 규율을 하고 있다는 특이점이 보이지 않는 상황임. 특히 미국은 생체정보의 보호보다는 활용측면에 다소 포커스가 맞춰져 있다고 평가됨
- 일반적 규율 - 개인정보보호에 관한 규율구조 - 의 틀에서 생체정보를 의율하고 있는 외국법제에 대한 의존 내지 연구 보다는 우리나라 상황에 맞춰 구체적인 보호 규정을 새롭게 만드는 입법 전략으로 나가는 것이 타당한 것 아닌가 하는 생각
- 결 : 외국법제의 일반적 내용을 우리 법제에 적용하는 것은 큰 의미가 없음

Ⅳ. 생체정보보호에 관한 입법전략의 수립

- 생체정보의 법리적 접근
 - 생체정보의 보호이익, 보호주체 등 헌법상 기본권 내용과 주체에 서의 접근
 - 관련 기본권을 열거하고 생체정보와 기본권 침해 관련성에 따른 보호영역을 파악

- ex) 개인정보자기결정권, 신체의 자유 등 케이스별 접근
- 생체정보가 노출되는 상황 사건에 대하여 현행 법률(개인정보보호법, 정보통신망법)을 적용하여 위험이 여전히 잔존하고 있는 영역을 발굴
- ex) 적용범위의 문제(생체정보의 범위), 행위태양의 공백(위반유형의 구체화), 위반행위자의 범위(법적용의무자의 선정), 실효성 없는 규제(제재수단의 미약) 등을 발굴
- 최근 이슈화된 사건 10개 이상을 선정하여, 실제 현행 법률을 적용시켜 규제공백 및 규제미비점을 발굴할 필요가 있음

○ 현행 규율 및 해외 입법례의 규제 구조 분석

○ 생체정보에 대한 생성주기별(생성, 이용, 전달, 유통, 폐기 등) 규제 현황 및 규제 필요부분 파악

ex) 생체정보의 규율 현황 파악 분석

	개인 정보 보호법	정보 통신망 법	EU 지침	독일	프랑스	일본
생체정보 개념						
생성 규제						
이용 규제						
전달 규제						

	개인 정보 보호법	정보 통신망 법	EU 지침	독일	프랑스	일본
폐기 규제						
:						
:						

○ 법체계 선택 (일반법의 부분조항으로 산입, 개별법률 신설 등)

- 일반법의 부분조항으로 산입 (개정 법률, 개정법률에 산입할 내용 등을 구체화)

ex) 생체정보의 개념, 생체정보의 특별한 보호, 생체정보관리자의 통제, 생체정보기기제조 규제, 생체정보이용자 규제, 제제수단 보충 등

- 개별법률 신설

ex) 생체정보보호의 목적 및 국가의 역할, 생체정보의 개념과 유형 구분, 생체정보이해관계자 개념정의(생성자, 관리자, 기기제조사, 이용자 등), 생체정보보호의 일반원칙, 타법률과의 관계, 생체정보보호 관리체계, 생체정보생성 및 유통과정에 따른 이해관계자 규제 및 행위규제, 기타 특별한 보호영역에 대한 규제, 실효성 확보 수단(제재 등), 보칙 으로 구성